计算机网络知识要点总结

一、现在最主要的三种网络

电信网络（电话网）

有线电视网络

计算机网络　(发展最快，信息时代的　核心 技术)

二、 **internet** 和 **Internet**

internet 是普通名词

泛指一般的互连网（互联网）

Internet 是专有名词 ,标准翻译是 “ 因特网 ”

世界范围的互连网（互联网）

使用　TCP/IP 协议族

前身是美国的阿帕网　　ARPANET

三、计算机网络的带宽

计算机网络的带宽是指网络可通过的最高数据率，即每秒多少比特。

描述带宽也常常把 “ 比特　/秒 ” 省略。

例如，带宽是　10 M，实际上是　10 Mb/s。注意：这里的　M 是 10^6。

四、对宽带传输的错误概念

在网络中有两种不同的速率：

信号（即电磁波）在传输媒体上的　　传播速率 （米 /秒，或公里 /秒）

计算机向网络发送比特的速率（比特　　/秒） ,也叫 传输速率。

这两种速率的意义和单位完全不同。

宽带传输：计算机　向网络发送比特的速率　较高。

宽带线路：每秒有更多比特从计算机注入到线路。

宽带线路和窄带线路上比特的传播速率是一样的。

早期的计算机网络采用　电路交换 ，新型的计算机网络采用　分组交换的、基于存储转发　的方式。

分组交换：

在发送端把要发送的报文分隔为较短的数据块

每个块增加带有控制信息的首部构成分组（包）

依次把各分组发送到接收端

接收端剥去首部，抽出数据部分，还原成报文

IP 网络的重要特点

每一个分组独立选择路由。

发往同一个目的地的分组，后发送的有可能先收到（即可能不按顺序接收）　　。

当网络中的通信量过大时，路由器就来不及处理分组，于是要丢弃一些分组。

因此，　IP 网络不保证分组的可靠地交付。

IP 网络提供的服务被称为：

尽最大努力服务　(best effort service)

五、最重要的两个协议：　**IP** 和 **TCP**

TCP 协议保证了应用程序之间的可靠通信　　,IP 协议控制分组在因特网的传输　　, 但因特网不保证可靠交

付.

在 TCP/IP 的应用层协议使用的是客户服务器方式。

客户 (client) 和服务器 (server)都是指通信中所涉及的两个应用进程。

客户服务器方式所描述的是进程之间服务和被服务的关系。

当 A 进程需要 B 进程的服务时就主动呼叫 B 进程，在这种情况下， A 是客户而 B 是服务器。

可能在下一次通信中， B 需要 A 的服务，此时， B 是客户而 A 是服务器。

注意：

使用计算机的人是“ 用户 ” (user)而不是“ 客户 ” (client) 。

客户和服务器都指的是进程，即计算机软件。

由于运行服务器进程的机器往往有许多特殊的要求，因此人们经常将主要运行服务器进程的机器（硬件）不严格地称为服务器。

例如，“ 这台机器是服务器。 ” 意思是：“ 这台机器（硬件）主要是用来运行服务器进程（软件） 。”

因此，服务器 (server)一词有时指的是软件，但也有时指的是硬件。

六、总结

因特网 (Internet) 是世界范围的、互连起来的计算机网络，它使用 TCP/IP 协议族，并且它的前身是美国阿帕网 ARPANET 。

计算机网络的带宽是网络可通过的 最高 数据率。

因特网使用 基于存储转发的分组交换 ，并使用 IP 协议传送 IP 分组。

路由器把许多网络互连起来，构成了互连网。路由器收到分组后，根据路由表查找出下一跳路由器的地址，然后转发分组。

路由器根据与其他路由器交换的路由信息构造出自己的路由表。

IP 网络提供尽最大努力服务，不保证可靠交付。

TCP 协议保证 计算机程序之间的、端到端 的可靠 交付。

在 TCP/IP 的应用层协议使用的是客户服务器方式。

客户和服务器都是进程（即软件） 。客户是服务请求方，服务器是服务提供方。

服务器有时也指“ 运行服务器软件 ”的机器。

==========

一、 **IP** 网络是虚拟网络

IP 网络是虚拟的。在 IP 网络上传送的是 IP 数据报（ IP 分组）。

实际上在网络链路上传送的是“ 帧 ” ，使用的是帧的硬件地址（ MAC 地址）。

地址解析协议 ARP 用来把 IP 地址（虚拟地址）转换为硬件地址（物理地址） 。

二、 **IP** 地址的表示方法

IP 地址的表示方法有两种： 二进制 和 点分十进制。

IP 地址是 32 位二进制数字，为方便阅读和从键盘上输入，可把每 8 位二进制数字转换成一个十进制数字，并用小数点隔开，这就是点分十进制。

三、因特网的域名

因特网的域名分为：

顶级域名

二级域名

三级域名

四级域名

四、 域名服务器 **DNS (Domain Name Server)**

因特网中设有很多的域名服务器 DNS，用来把域名转换为 IP 地址。

五、 电子邮件

发送邮件使用的协议——简单邮件传送协议 SMTP (Simple Mail Transfer Protocol)

接收邮件使用的协议——邮局协议版本 3 POP3 (Post Office Protocol version 3)

注：邮件的传送仍然要使用 IP 和 TCP 协议

六、统一资源定位符 **URL (Uniform Resource Locator)**

URL 用来 标识万维网上的各种文档 。

因特网上的每一个文档，在整个因特网的范围内具有惟一的标识符 URL 。

URL 实际上就是文档在因特网中的 地址 。

七、超文本传送协议 **HTTP (HyperText Transfer Protocol)**

万维网客户程序与服务器程序之间的交互遵守超文本传送协议 HTTP 。

八、结束语

IP 地址是 32 位二进制数字。为便于阅读和键入，也常使用点分十进制记法。

个人用户上网可向本地 ISP 租用临时的 IP 地址。

域名服务器 DNS 把计算机域名转换为计算机使用的 32 位二进制 IP 地址。

发送电子邮件使用 SMTP 协议，接收电子邮件使用 POP3 协议。

统一资源定位符 URL 惟一地确定了万维网上文档的地址。

超文本传送协议 HTTP 用于万维网浏览器程序和服务器程序的信息交互。

超文本标记语言 HTML 使万维网文档有了统一的格式。

IP 电话不使用 TCP 协议。利用 IP 电话网关使得在普通电话之间可以打 IP 电话。

==========

一、 因特网服务提供者 **ISP (Internet Service Provider)**

根据提供服务的覆盖面积大小以及所拥有的 IP 地址数目的不同， ISP 也分成为不同的层次。

二、 两种通信方式

在网络边缘的端系统中运行的程序之间的通信方式通常可划分为两大类： C/S 方式 和 P2P 方式（Peer-to-Peer，对等方式）。

三、 因特网的核心部分

网络核心部分是因特网中最复杂的部分。

网络中的核心部分要向网络边缘中的大量主机提供连通性，使边缘部分中的任何一个主机都能够向其他主机通信（即传送或接收各种形式的数据） 。

因特网的核心部分是由许多 网络 和把它们互连起来的 路由器 组成，而 主机处在因特网的边缘部分 。

在因特网核心部分的路由器之间一般都用高速链路相连接，而在网络边缘的主机接入到核心部分则通常以相对较低速率的链路相连接。

主机 的用途是为用户进行信息处理的，并且可以和其他主机通过网络交换信息。 路由器 的用途则是用来转发分组的，即进行分组交换的。

在网络核心部分起 特殊作用 的是 路由器 (router)。

路由器是实现 分组交换 (packet switching) 的关键构件，其任务是 转发收到的分组 ，这是网络核心部分最重要的功能。

四、 电路交换

电路交换必定是 面向连接 的。

电路交换的三个阶段： 建立连接 、通信、 释放连接 。

五、 网络的分类

不同作用范围的网络

广域网 WAN (Wide Area Network)

局域网 LAN (Local Area Network)

城域网 MAN (Metropolitan Area Network)

个人区域网 PAN (Personal Area Network)

从网络的使用者进行分类

公用网 (public network)

专用网 (private network)

用来把用户接入到因特网的网络

接入网 AN (Access Network) ，它又称为本地接入网或居民接入网。

注：由 ISP 提供的接入网只是起到让用户能够与因特网连接的“ 桥梁 ”作用。

六、计算机网络的性能指标

速率

带宽

吞吐量

时延 (delay 或 latency)

传输时延 （发送时延 ）—— 从发送数据帧的第一个比特算起， 到该帧的最后一个比特发送完毕所需的时间。

传播时延 —— 电磁波在信道中需要传播一定的距离而花费的时间。

注：信号传输速率（即发送速率）和信号在信道上的传播速率是完全不同的概念。

处理时延 —— 交换结点为存储转发而进行一些必要的处理所花费的时间。

排队时延 —— 结点缓存队列中分组排队所经历的时延。

总时延 = 发送时延 +传播时延 +处理时延 +处理时延

时延带宽积

利用率 —— 分为 信道利用率 和 网络利用率 。

信道利用率——某信道有百分之几的时间是被利用的（有数据通过）　　。

网络利用率——全网络的信道利用率的加权平均值。

注：信道利用率并非越高越好。

七、 网络协议 **(network protocol)**

简称为 协议 ， 是为进行网络中的数据交换而建立的规则、标准或约定。其组成要素有以下三点：

语法　　数据与控制信息的结构或格式　　。

语义　　需要发出何种控制信息，完成何种动作以及做出何种响应。

同步　　事件实现顺序的详细说明。

八、实体、协议、服务和服务访问点

实体 (entity) ——表示任何可发送或接收信息的硬件或软件进程。

协议—— 是控制两个 对等 实体进行 通信 的规则的集合。

在协议的控制下，两个对等实体间的通信使得本层能够向上一层提供服务。

要实现本层协议，还需要使用下层所提供的服务。

本层的服务用户只能看见服务而无法看见下面的协议。

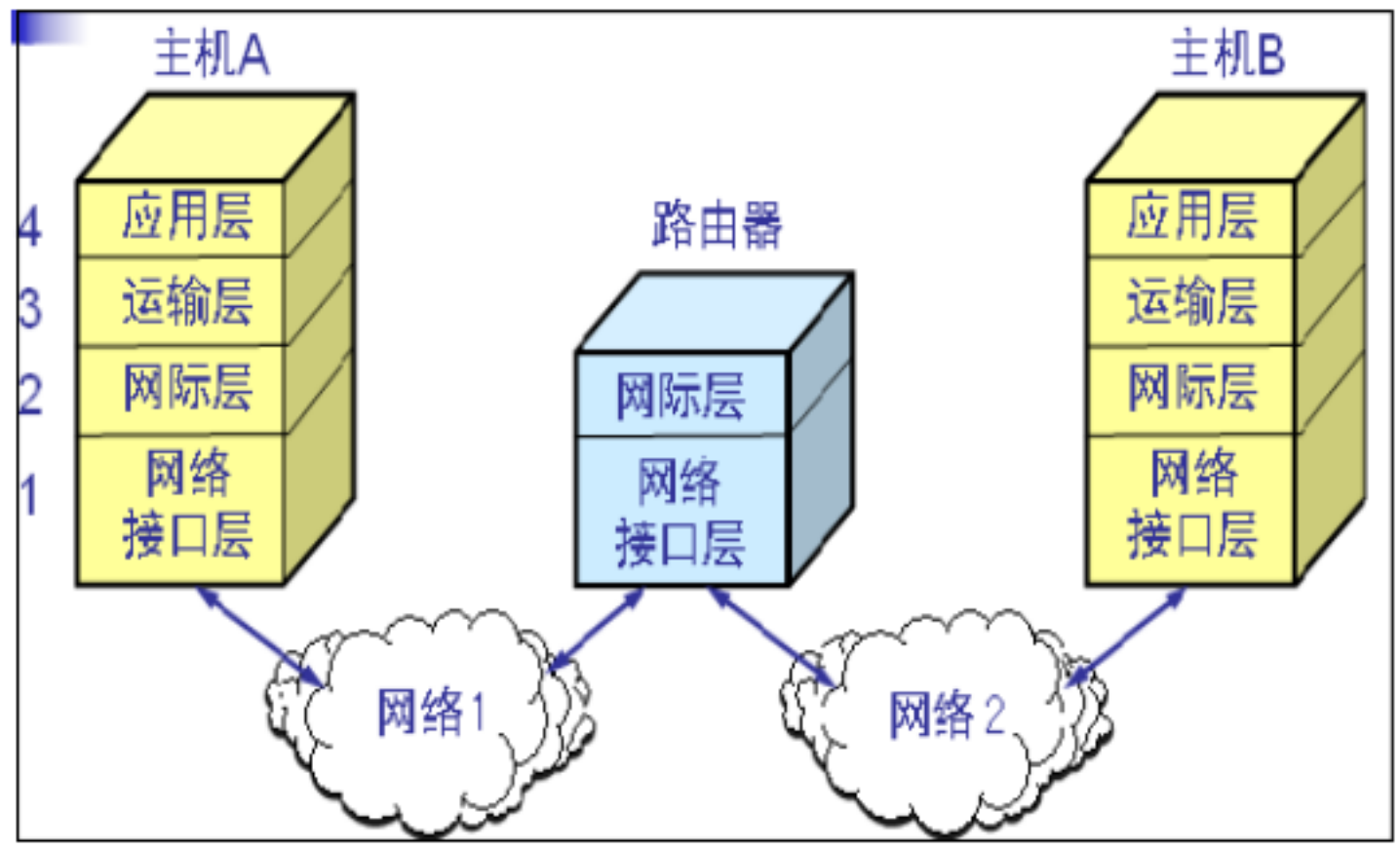
下面的协议对上面的服务用户是透明的。

协议是“ 水平的 ” ，即协议是控制对等实体之间通信的规则。

服务是“ 垂直的 ” ，即服务是 由下层向上层 通过层间接口提供的。

同一系统 相邻两层 的实体进行 交互 的地方，称为 服务访问点　SAP (Service Access Point)。

九、 **TCP/IP** 的体系结构



路由器 在转发分组时　最高 只用到 网络层 ， 而没有使用运输层和应用层。

==========

第二章　物理层

一、物理层的基本概念

物理层的主要任务是　确定与传输媒体的接口的一些特性　，即：

机械特性 ——指明接口所用接线器的形状和尺寸、引线数目和排列、固定和锁定装置等等。

电气特性 ——指明在接口电缆的各条线上出现的电压的范围。

功能特性 ——指明某条线上出现的某一电平的电压表示何种意义。

过程特性 ——指明对于不同功能的各种可能事件的出现顺序。

二、几个术语

数据 (data)——运送消息的实体。

信号 (signal)——数据的电气的或电磁的表现。

“ 模拟的 ”(analogous)——代表消息的参数的取值是　连续 的。

“ 数字的 ”(digital) ——代表消息的参数的取值是　离散 的。

码元 (code)——在使用时间域（或简称为时域）的波形表示数字信号时，代表不同离散数值的　基本波形 。

三、　有关信号的几个基本概念

单向通信（ 单工通信 ）——只能有一个方向的通信而没有反方向的交互。

双向交替通信（ 半双工通信 ）——通信的双方都可以发送信息，但不能双方同时发送　(当然也就不能同时接收)。

双向同时通信（ 全双工通信 ）——通信的双方可以同时发送和接收信息。

四、基带信号和调制

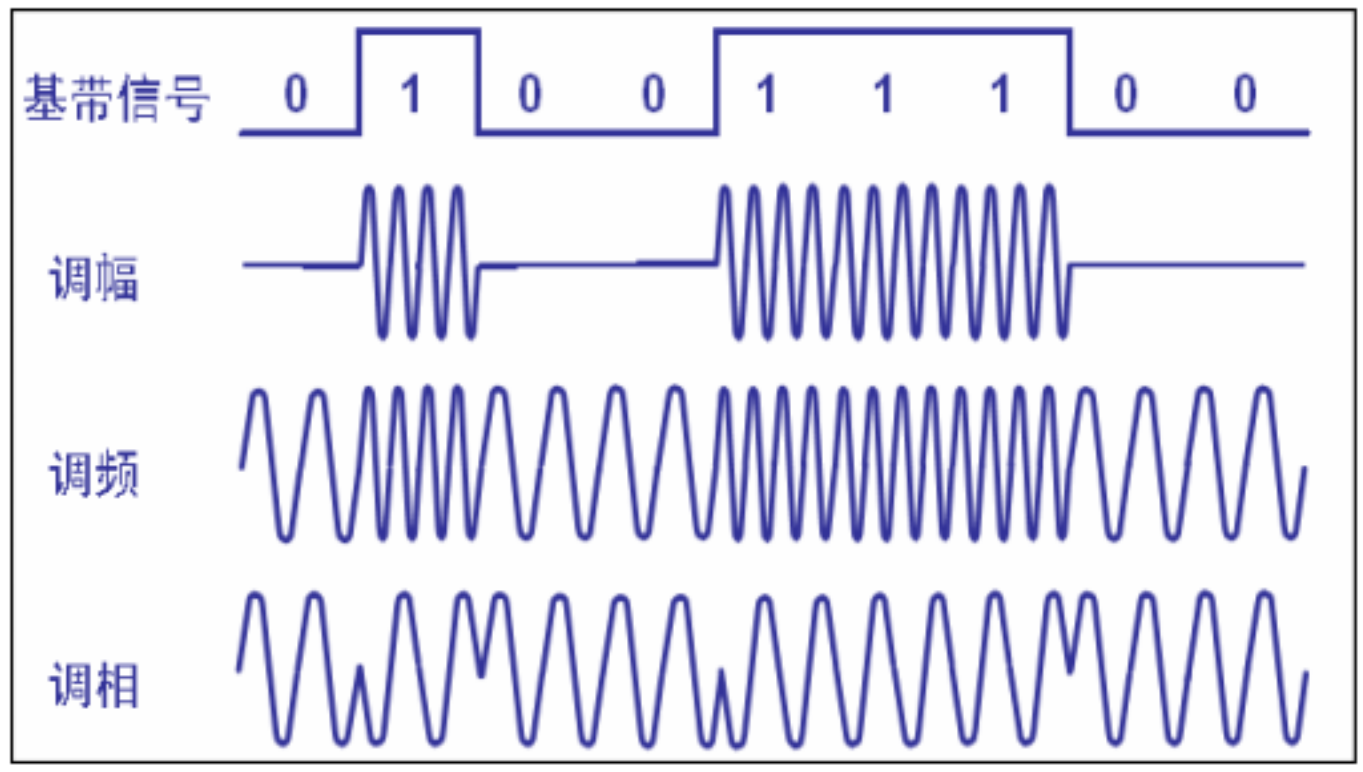
基带信号往往包含有较多的低频成分，甚至有直流成分，而许多信道并不能传输这种低频分量或直流分量。为了解决这一问题，就必须对基带信号进行　调制 (modulation) 。

最基本的二元制调制方法有以下几种：

调幅 (AM) ：载波的振幅随基带数字信号而变化。

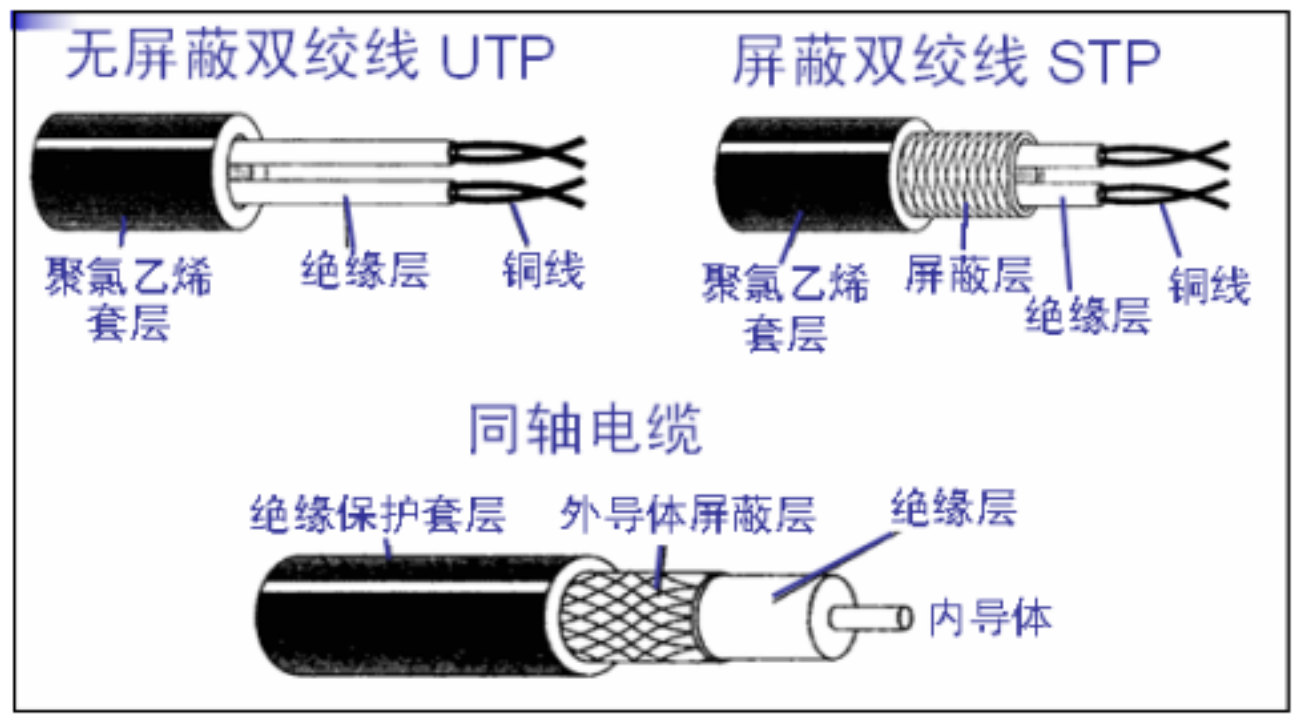
调频 (FM) ：载波的频率随基带数字信号而变化。

调相 (PM):　载波的初始相位随基带数字信号而变化。



五、导向传输媒体

双绞线、同轴电缆、光缆　　、无线信道 。



六、信道复用技术

复用 (multiplexing) 是通信技术中的基本概念。

复用技术的分类：

频分复用　FDM(Frequency Division Multiplexing)

时分复用　TDM(Time Division Multiplexing)

波分复用　WDM(Wavelength Division Multiplexing)

码分复用　CDM(Code Division Multiplexing)

常用的名词是 码分多址 CDMA (Code Division Multiple Access) 。

各用户使用经过特殊挑选的不同码型，因此彼此不会造成干扰。

这种系统发送的信号有　很强的抗干扰能力　，其频谱类似于白噪声，不易被敌人发现。

每一个比特时间划分为 m 个短的间隔，称为 码片 (chip)。

码片序列 **(chip sequence)**

每个站被指派一个唯一的 m bit 码片序列。

如发送比特 1，则发送自己的 m bit 码片序列 。

如发送比特 0，则发送该码片序列的 二进制反码 。

例如， S 站的 8 bit 码片序列是 00011011。

发送比特 1 时，就发送序列 00011011，

发送比特 0 时，就发送序列 11100100。

每个站分配的码片序列不仅必须各不相同，并且还必须互相正交 (orthogonal) 。

两个不同站的码片序列 正交 , 就是向量 **S** 和 **T** 的规格化 内积 **(inner product)** 都是 **0**：

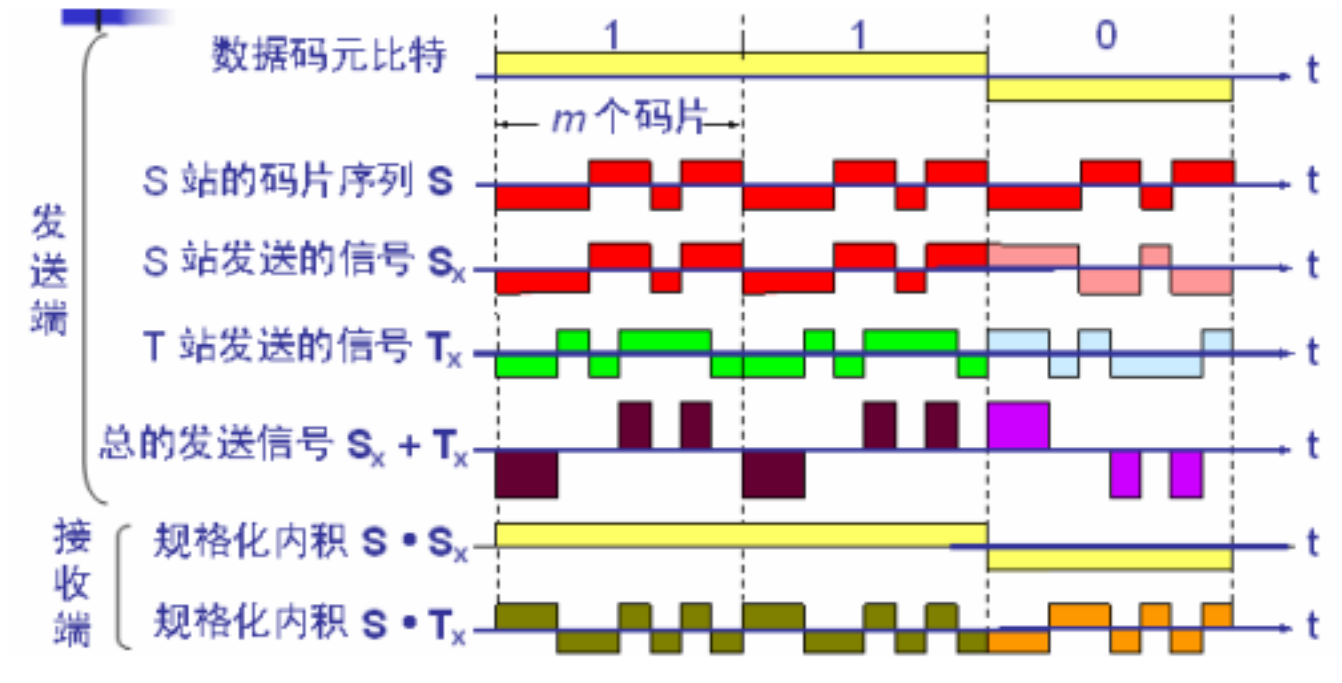
$$\mathbf{S} \bullet \mathbf{T} \equiv \frac{1}{m} \sum_{i=1}^{m} S_i T_i = 0$$

任何一个码片向量和该码片向量自己的规格化内积都是 **1** ：

$$\mathbf{S} \bullet \mathbf{S} = \frac{1}{m} \sum_{i=1}^{m} S_i S_i = \frac{1}{m} \sum_{i=1}^{m} S_i^2 = \frac{1}{m} \sum_{i=1}^{m} (\pm 1)^2 = 1$$

一个码片向量和该码片反码的向量的规格化内积值是 **－1**。

CDMA 的工作原理



==========

第 3 章　数据链路层

一、数据链路层使用的信道分类

数据链路层使用的信道主要有以下两种类型：

点对点信道　：这种信道使用一对一的点对点通信方式。

广播信道　：这种信道使用一对多的广播通信方式，因此过程比较复杂。

二、各层传输的数据单位

网络层：　IP 数据报（或　IP 分组）

数据链路层：帧

物理层：比特

三、数据链路层传输数据时的三个基本问题

(1)　封装成帧 (framing) ——在一段数据的前后分别添加首部和尾部，然后就构成了一个帧。首部和尾部的一个重要作用就是进行帧定界。

(2)　透明传输

(3)　差错控制

四、点对点协议　**PPP (Point-to-Point Protocol)**

现在全世界　使用得最多的数据链路层协议　是点对点协议　PPP。用户使用　拨号电话线接入因特网时，一般都是　使用　PPP 协议。

1. PPP 协议应满足的需求

简单 ——这是首要的要求

封装成帧

透明性

多种网络层协议

多种类型链路

差错检测

检测连接状态

最大传送单元

网络层地址协商

数据压缩协商

2. PPP 协议不需要的功能

纠错 (只需要检测有无错，而不需纠错)

流量控制

序号

多点线路

半双工或单工链路

3.PPP 协议有三个组成部分

1) 一个将 IP 数据报封装到串行链路的方法。

2) 链路控制协议 LCP (Link Control Protocol) 。

3) 网络控制协议 NCP (Network Control Protocol) 。

4.PPP 协议之 不使用序号和确认机制 .

五、媒体共享技术

1. 静态划分信道

1) 频分复用

2) 时分复用

3) 波分复用

4) 码分复用

2. 动态媒体接入控制（多点接入）

1) 随机接入

2) 受控接入 ，如多点线路探询 (polling)，或轮询。

六、以太网的两个标准

DIX Ethernet V2 标准与 IEEE 的 802.3 标准只有很小的差别，因此可以将 802.3 局域网简称为“以太网”。

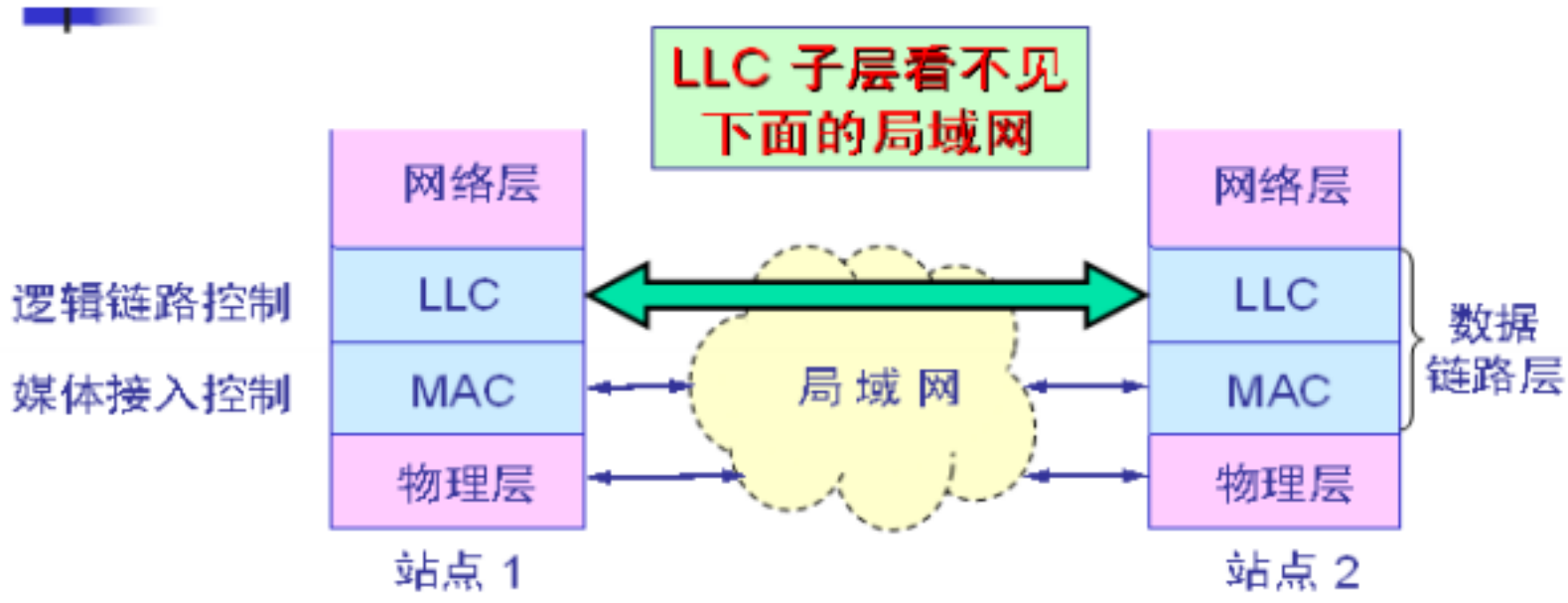
七、数据链路层的两个子层

逻辑链路控制 LLC (Logical Link Control) 子层

媒体接入控制 MAC (Medium Access Control) 子层。

与接入到传输媒体有关的内容都放在 MAC 子层，而 LLC 子层则与传输媒体无关，不管采用何

种协议的局域网对　　LLC　子层来说都是透明的　,如下图所示：



局域网对　LLC　子层是透明的

注意 ：

1. 由于　TCP/IP　体系经常使用的局域网是　　DIX Ethernet V2　而不是　802.3　标准中的几种局域网，　因此现在　802　委员会制定的逻辑链路控制子层　　LLC （即　802.2　标准）的作用已经不大了。
2. 很多厂商生产的适配器上就仅装有　　MAC　协议而没有　LLC　协议。
3. 所以我们以后一般不考虑　　LLC　子层　。

八、以太网提供的服务

以太网提供的服务是不可靠的交付，即尽最大努力的交付。

当目的站收到有差错的数据帧时就丢弃此帧，其他什么也不做。　　差错的纠正由高层来决定　。

如果高层发现丢失了一些数据而进行重传，但以太网并不知道这是一个重传的帧，而是当作一个新的数据帧来发送。

以太网发送的数据都使用曼彻斯特　　(Manchester) 编码 。

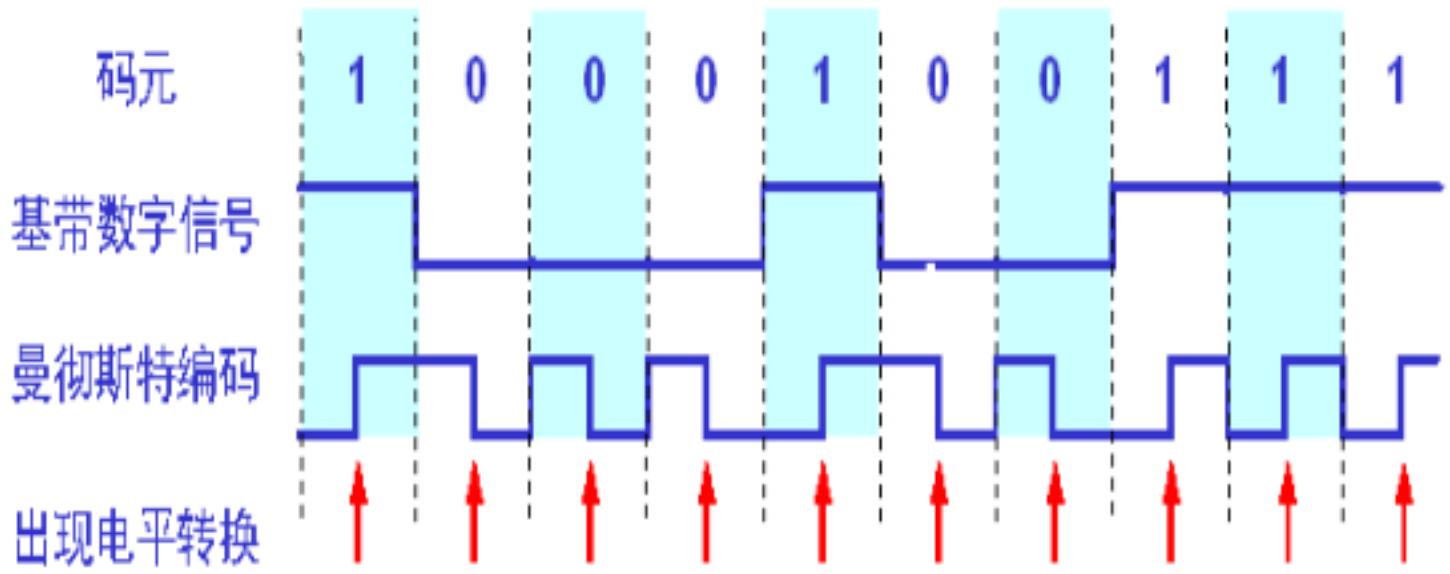


图　曼彻斯特编码方式

九、载波监听多点接入　/冲突检测（ **CSMA/CD** ）

CSMA/CD 表示 Carrier Sense Multiple Access with Collision Detection 。

“多点接入”表示 许多计算机以多点接入的方式连接在一根总线上 。

“载波监听”是指每一个站在发送数据之前先要检测一下总线上是否有其他计算机在发送数据，

如果 有，则暂时不要发送数据，以免发生碰撞。

总线上并没有什么“载波” 。因此， “载波监听”就是用电子技术检测总线上有没有其他计算机发送的数据信号。

“冲突检测”就是计算机边发送数据边检测信道上的信号电压大小。

当几个站同时在总线上发送数据时，总线上的信号电压摆动值将会增大（互相叠加） 。

当一个站检测到的信号电压摆动值超过一定的门限值时，就认为总线上至少有两个站同时在发送数据，表明产生了冲突。

检测到碰撞后

在发生碰撞时，总线上传输的信号产生了严重的失真，无法从中恢复出有用的信息来。

每一个正在发送数据的站，一旦发现总线上出现了碰撞，就要立即停止发送，免得继续浪费网络资源，然后等待一段随机时间后再次发送。

重要特性

使用 CSMA/CD 协议的以太网不能进行全双工通信而只能进行 双向交替通信（半双工通信 ）。

每个站在发送数据之后的一小段时间内，存在着遭遇碰撞的可能性。

这种发送的不确定性使整个以太网的平均通信量远小于以太网的最高数据率。

十、以太网的 MAC 层

1、**48** 位的 **MAC** 地址

在局域网中，硬件地址又称为物理地址，或 MAC 地址，共 48 位，其前 3 个字节（即高 24 位）用于标识不同的生产厂家，后 3 个字节（即低 24 位）由厂家自行指派，用于标识产品号。

2、从网络上发往本站的帧分为以下 **3** 种**:**

1) 单播 (unicast)帧（一对一）

2) 广播 (broadcast)帧（一对全体）

3) 多播 (multicast) 帧（一对多）

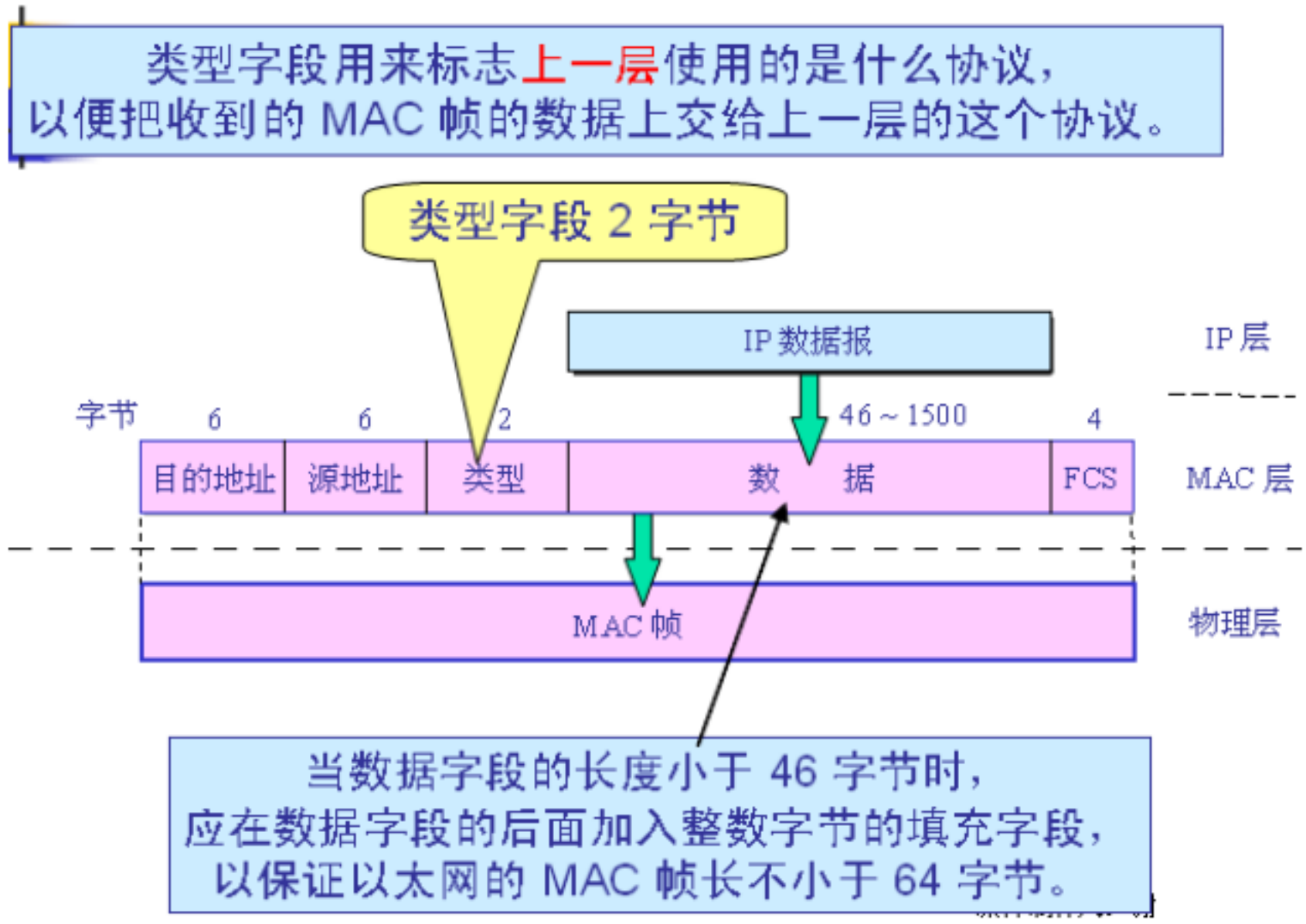
3、 **MAC** 帧的格式

常用的以太网 MAC 帧格式有两种标准 ：

1) DIX Ethernet V2 标准

2) IEEE 的 802.3 标准

最常用的　MAC　帧是 以太网　V2　的格式 ,如下：



4、帧间最小间隔

帧间最小间隔为　9.6　s，相当于　96 bit　的发送时间。

一个站在检测到总线开始空闲后，还要等待　9.6　s　才能再次发送数据。

这样做是为了使刚刚收到数据帧的站的接收缓存来得及清理，做好接收下一帧的准备。

5、 多接口网桥——以太网交换机

以太网交换机通常都有十几个接口。因此，以太网　交换机实质上就是一个多接口的网桥，可见 交换机工作在数据链路层　。

以太网 交换机 的每个接口都直接与主机相连，并且一般都工作在　全双工方式　。

交换机能同时连通许多对的接口，使　每一对相互通信的主机都能像独占通信媒体　那样，进行无碰撞地传输数据。

以太网交换机由于使用了专用的交换结构芯片，其交换速率就较高。

十一、虚拟局域网

虚拟局域网　VLAN　是由一些局域网网段构成的与物理位置无关的逻辑组。

这些网段具有某些共同的需求。

每一个 VLAN 的帧都有一个明确的标识符，指明发送这个帧的工作站是属于哪一个 VLAN 。

虚拟局域网其实只是局域网给用户提供的一种服务，而并不是一种新型局域网。

虚拟局域网限制了接收广播信息的工作站数，使得网络不会因传播过多的广播信息(即“ 广播风暴 ”)而引起性能恶化。

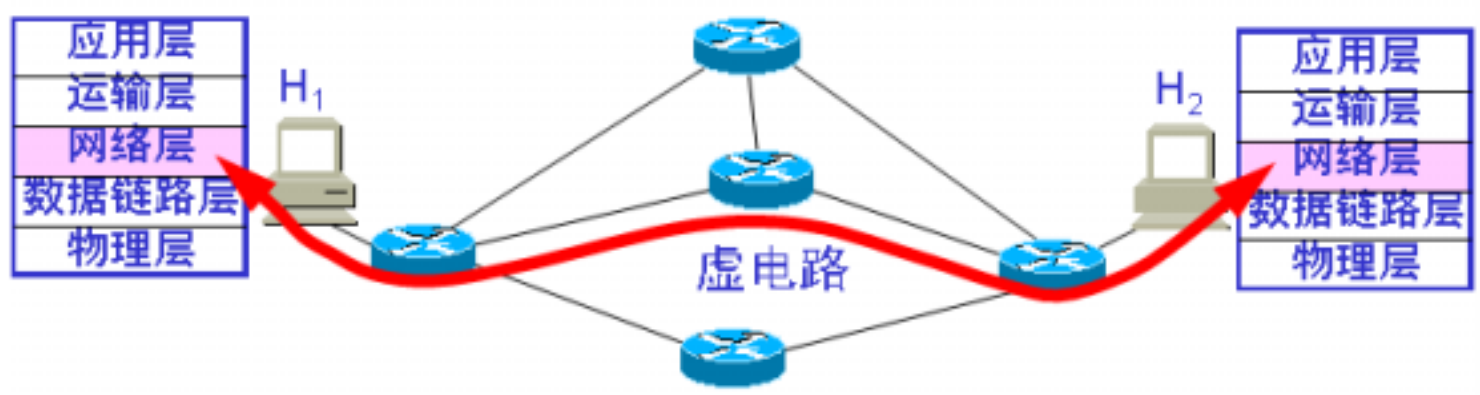
虚拟局域网协议允许在以太网的帧格式中插入一个 4 字节的标识符，称为 VLAN 标记(tag)，用来指明发送该帧的工作站属于哪一个虚拟局域网。

十二、 网络层提供的两种服务

网络层提供两种类型的的服务，即： 虚电路服务 和数据报服务 。

面向连接的通信方式

建立虚电路 (Virtual Circuit) ，以保证双方通信所需的一切网络资源。



图示 虚电路服务

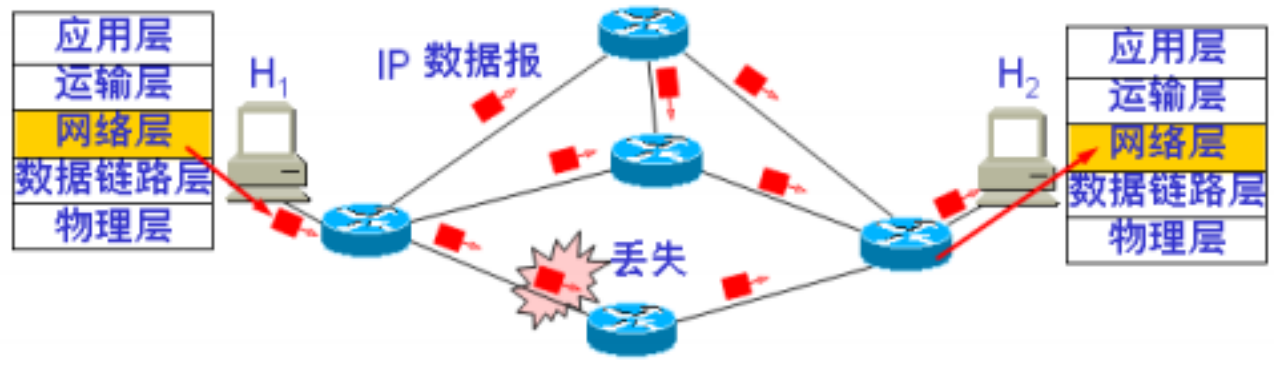
虚电路表示这只是一条 逻辑上的连接 ，分组都沿着这条逻辑连接按照存储转发方式传送，而并不是真正建立了一条物理连接。

请注意，电路交换的 电话通信 是先建立了一条 真正的连接 。因此分组交换的虚连接和电路交换的连接只是类似，但并不完全一样。

如果再使用可靠传输的网络协议，就可使所发送的分组无差错按序到达终点。

无连接的通信方式

网络层向上只提供简单灵活的、 无连接的 、尽最大努力交付的 数据报服务 。



H_1 发送给 H_2 的分组可能沿着不同路径传送

图示　数据报服务

十三、网际协议　**IP**

网际协议　IP　是　TCP/IP　体系中两个最主要的协议之一。与　　IP　协议配套使用的还有四个协议：

地址解析协议　ARP (Address Resolution Protocol)

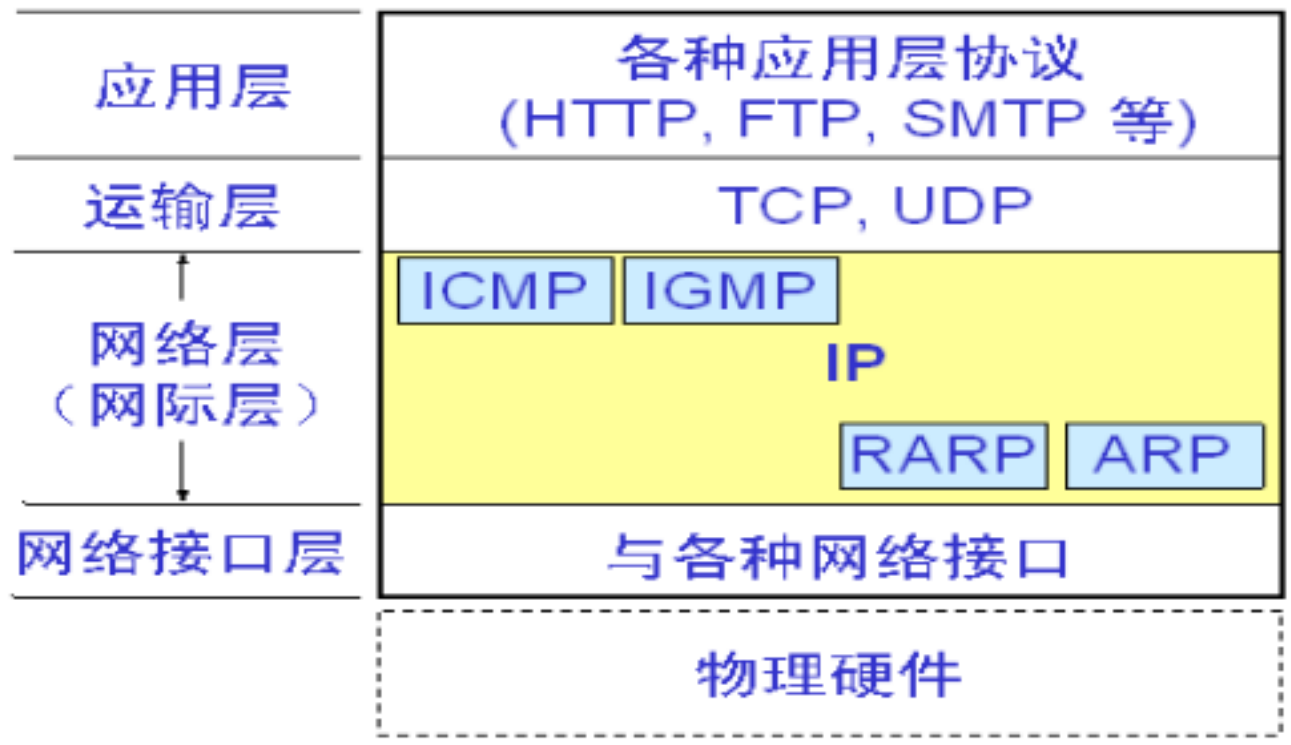
逆地址解析协议　RARP (Reverse Address Resolution Protocol)

网际控制报文协议　ICMP (Internet Control Message Protocol)

注：ICMP　不是高层协议，而是　　IP　层的协议。

网际组管理协议　IGMP (Internet Group Management Protocol)

十四、网际层的　**IP**　协议及配套协议



注：ICMP　网际控制报文协议

十五、网络互相连接起来要使用一些中间设备

中间设备又称为中间系统或中继　　(relay)系统。

物理层 中继系统：　转发器 (repeater)、中继器。

数据链路层　中继系统：　网桥 或 桥接器 (bridge)。

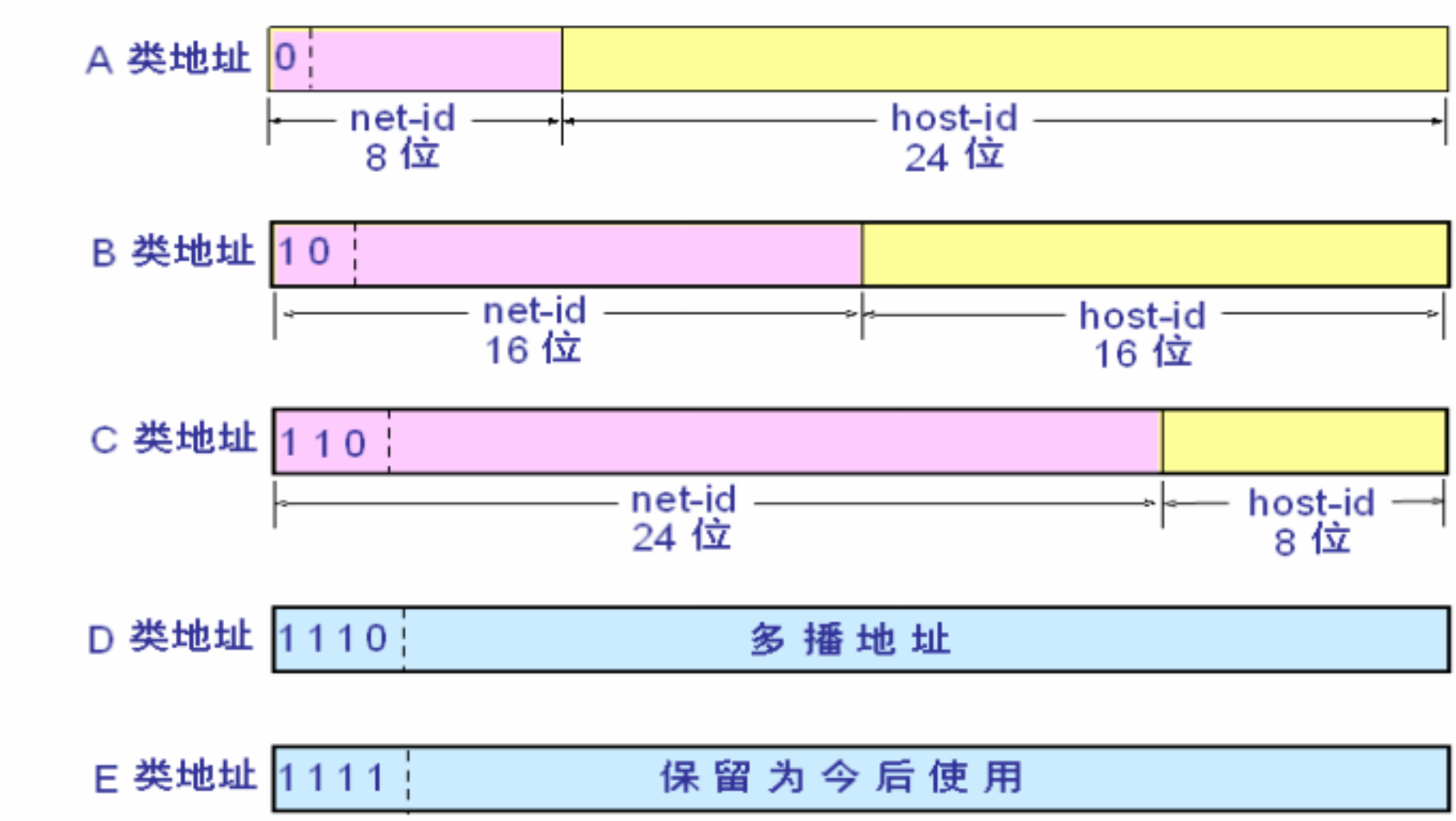
网络层 中继系统： 路由器 (router)。
网桥和路由器的混合物：桥路器 (brouter)。
网络层以上 的中继系统： 网关 (gateway)。

十六、网络互连使用路由器

当中继系统是转发器或网桥时，一般并不称之为网络互连，因为这仅仅是把一个网络扩大了，而这仍然是一个网络 。
网关由于比较复杂，目前使用得较少。
互联网都是指用路由器进行互连的网络 。
由于历史的原因，许多有关 TCP/IP 的文献将网络层使用的 路由器称为网关 。
路由器总是具有 两个或两个以上 的 IP 地址。
路由器的每一个接口都有一个 不同网络号 的 IP 地址。

十七、分类 IP 地址

每一类地址都由两个固定长度的字段组成，其中一个字段是网络号 net-id，它标志主机（或路由器）所连接到的网络，而另一个字段则是主机号 host-id，它标志该主机（或路由器） 。
两级的 IP 地址可以记为： IP 地址 ::= { < 网络号 >, < 主机号 >} ， ::= 代表“ 定义为 ”



IP 地址中的网络号字段和主机号字段

常用的三种类别的 IP 地址

网络类别	最大网络数	第一个可用的网络号	最后一个可用的网络号	每个网络中最大的主机数
A	126 ($2^7 - 2$)	1	126	16,777,214
B	16,383($2^{14} - 1$)	128.1	191.255	65,534
C	2,097,151 ($2^{21} - 1$)	192.0.1	223.255.255	254

IP 地址的一些重要特点

(1) IP 地址是一种分等级的地址结构

(2) 实际上 IP 地址是标志一个主机（或路由器）和一条链路的接口。

当一个主机同时连接到两个网络上时，该主机就必须同时具有两个相应的 IP 地址，其网络号 net-id 必须是不同的。这种主机称为多归属主机 (multihomed host) 。

由于一个路由器至少应当连接到两个网络（这样它才能将 IP 数据报从一个网络转发到另一个网络），因此 一个路由器至少应当有两个不同的 IP 地址 。

(3) 用转发器或 网桥连接 起来的若干个局域网 仍为一个网络 ，因此这些局域网都具有同样的网络号 net-id 。

(4) 所有分配到网络号 net-id 的网络，无论是范围很小的局域网，还是可能覆盖很大地理范围的广域网，都是平等的。

十八、 IP 地址与硬件地址

网络层及以上使用 IP 地址

路由器只根据目的站的 IP 地址的 网络号 进行路由选择

链路层及以下使用 MAC 地址

在具体的物理网络的链路层只能看见 MAC 帧而看不见 IP 数据报

十九、地址解析协议 ARP 和逆地址解析协议 RARP

1、 ARP

不管网络层使用的是什么协议， 在实际网络的链路上传送数据帧时， 最终还是必须使用硬件地址。

每一个主机都设有一个 ARP 高速缓存 (ARP cache)，里面有所在的局域网上的各主机和路由器的 IP 地址到硬件地址的映射表。

当主机 A 欲向本局域网上的某个主机 B 发送 IP 数据报时， 就先在其 ARP 高速缓存中查看有无主机 B 的 IP 地址。如有，就可查出其对应的硬件地址，再将此硬件地址写入 MAC 帧，然后通过局域网将该 MAC 帧发往此硬件地址。

ARP 是解决 同一个局域网 上的主机或路由器的 IP 地址和硬件地址的映射问题。

如果所要找的主机和源主机不在同一个局域网上，那么就要通过 ARP 找到一个位于本局域网上的某个路由器的硬件地址，然后把分组发送给这个路由器，让这个路由器把分组转发给下一个网络。剩下的工作就由下一个网络来做。

2、 RARP

逆地址解析协议 RARP 使只知道自己硬件地址的主机能够知道其 IP 地址。

这种主机往往是无盘工作站。 因此 RARP 协议目前已很少使用。

二十、查找路由表

在路由表中，对每一条路由，最主要的是（　　目的网络地址　，　下一跳地址　）.

根据目的网络地址就能确定下一跳路由器，这样做的结果是：

IP 数据报最终一定可以找到目的主机所在目的网络上的路由器（可能要通过多次的间接交付）。

只有到达最后一个路由器时，才试图向目的主机进行直接交付。

二十一、划分子网 **(subnetting)**

从 1985 年起在 IP 地址中又增加了一个“ 子网号字段 ” ，使两级的 IP 地址变成为 三级的 IP 地址。这种做法叫作划分子网 (subnetting) 。划分子网已成为因特网的正式标准协议。

划分子网纯属一个 单位内部的事情 。单位对外仍然表现为没有划分子网的网络。

从主机号 借用若干个位 作为 子网号 subnet-id，而主机号 host-id 也就相应减少了若干个位。

IP 地址 ::= {< 网络号 >, <子网号 >, <主机号 >}

凡是从其他网络发送给本单位某个主机的 IP 数据报，仍然是根据 IP 数据报的目的网络号 net-id，先找到连接在本单位网络上的路由器。

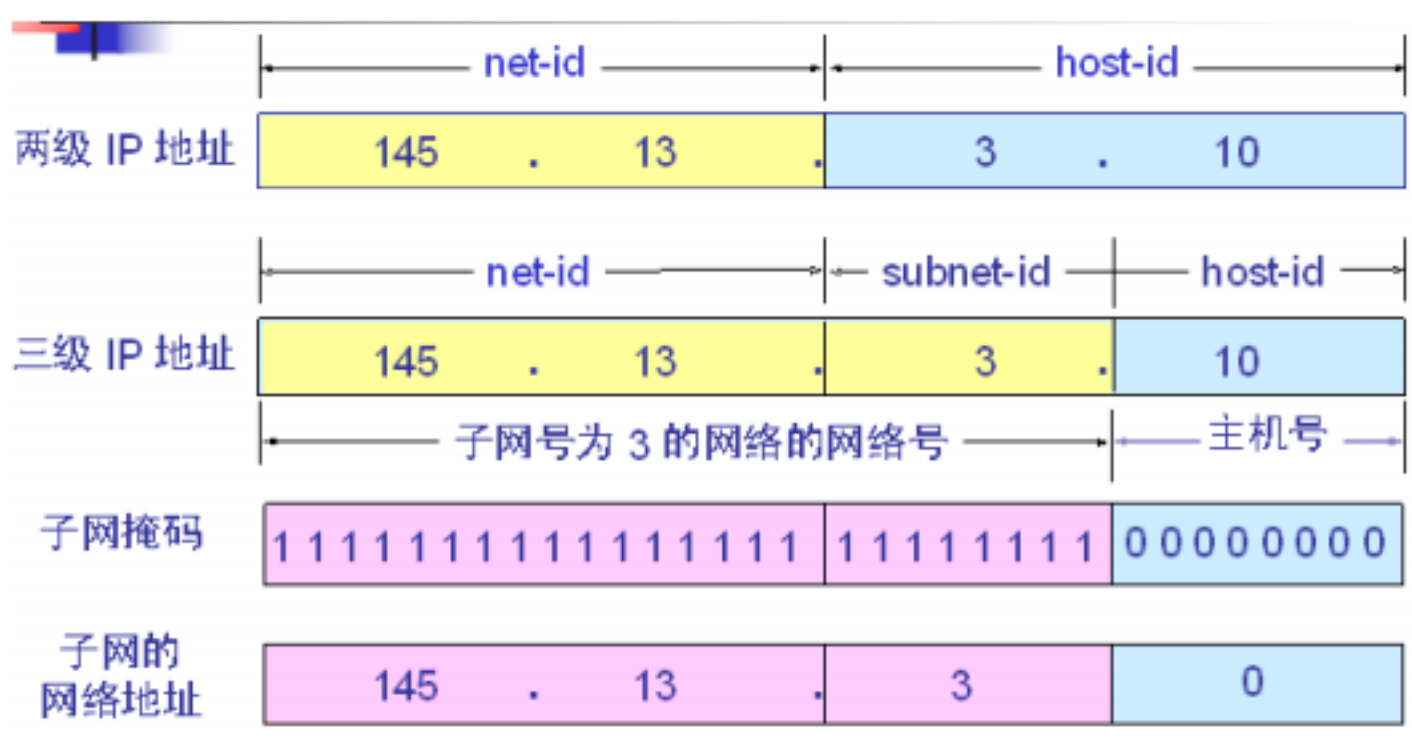
然后此路由器在收到 IP 数据报后，再按目的网络号 net-id 和子网号 subnet-id 找到目的子网。

最后就将 IP 数据报直接交付目的主机。

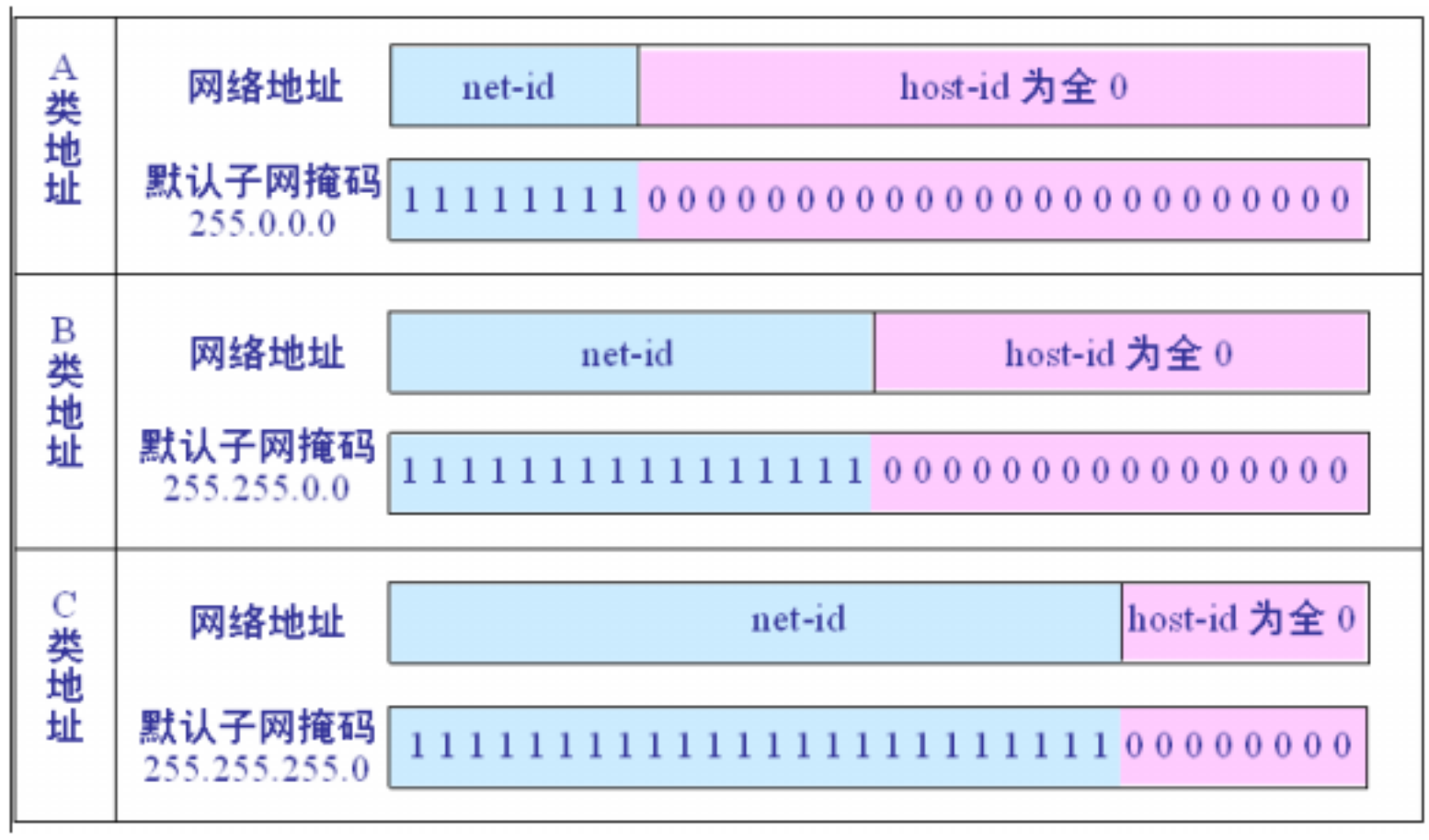
子网掩码

从一个 IP 数据报的首部并 无法判断 源主机或目的主机所连接的网络是否进行了子网划分。

使用 子网掩码 (subnet mask)可以找出 IP 地址中的子网部分。



IP 地址的各字段和子网掩码



默认子网掩码

二十二、因特网的路由选择协议

1、 有关路由选择协议的几个基本概念 **：**

1) 理想的路由算法

算法必须是正确的和完整的。

算法在计算上应简单。

算法应能适应通信量和网络拓扑的变化，这就是说，要有自适应性。

算法应具有稳定性。

算法应是公平的。

算法应是最佳的。

2、 关于“ 最佳路由 ”

不存在一种绝对的最佳路由算法 。

所谓“ 最佳 ”只能是相对于某一种特定要求下得出的较为合理的选择而已。

实际的路由选择算法，应尽可能接近于理想的算法。

路由选择是个非常复杂的问题

它是网络中的所有结点共同协调工作的结果。

路由选择的环境往往是不断变化的，而这种变化有时无法事先知道。

3、 从路由算法的自适应性考虑：

静态路由选择策略—　—即非自适应路由选择，其特点是简单和开销较小，但不能及时适应网络状态的变化。

动态路由选择策略　——即自适应路由选择，其特点是能较好地适应网络状态的变化，但实现起来较为复杂，开销也比较大。

4、因特网中的两大类路由选择协议：

内部网关协议　IGP (Interior Gateway Protocol) ——即在一个自治系统内部使用的路由选择协议。目前这类路由选择协议使用得最多，其具体的协议有多种，如　　RIP 和 OSPF 协议：

RIP: Routing Information Protocol　路由信息协议

→　RIP 协议的三个要点：

仅和 相邻路由器 交换信息。

交换的信息是当前本路由器所知道的　　全部信息 ，即自己的路由表。

按固定的时间间隔　交换路由信息，例如，每隔　　30 秒。

OSPF：Open Shortest Path First　开放最短路径优先

外部网关协议　EGP (External Gateway Protocol) ——　若源站和目的站处在不同的自治系统中，当数据报传到一个自治系统的边界时，就需要使用一种协议将路由选择信息传递到另一个自治系统中。 这样的协议就是外部网关协议　　EGP。在外部网关协议中目前使用最多的是　　BGP-4。

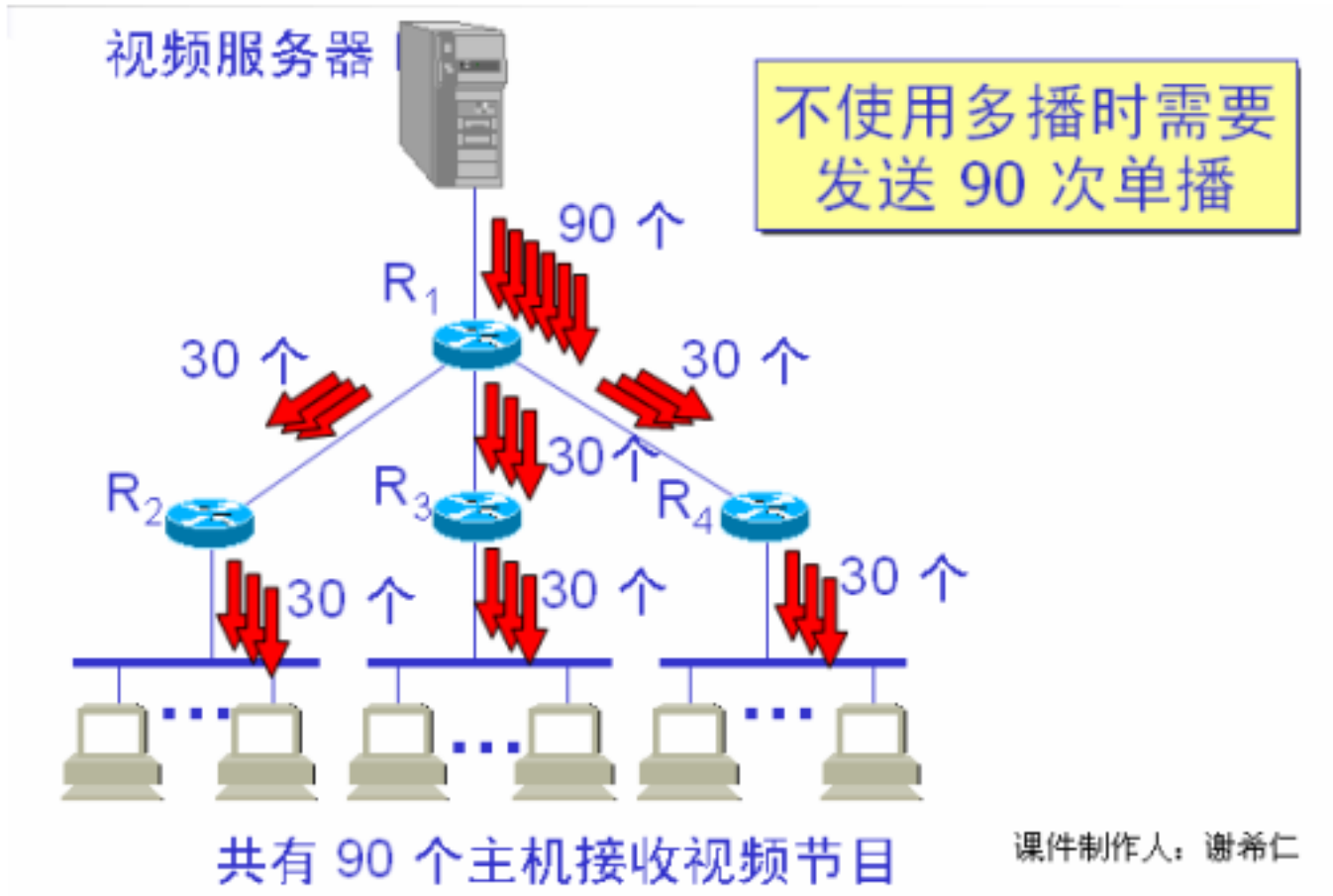
BGP ：Border Gateway Protocol　边界网关协议

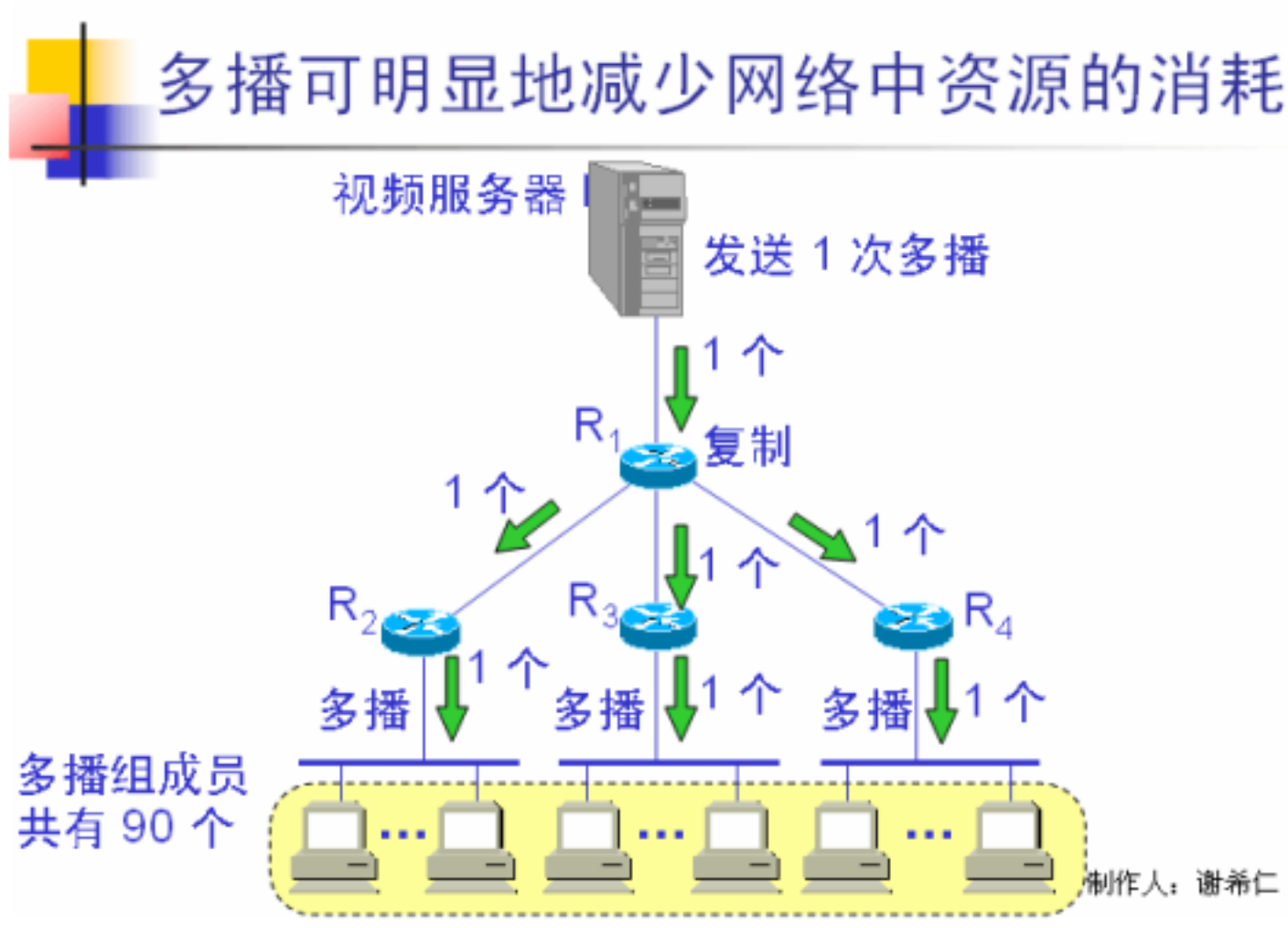
BGP 是不同自治系统的路由器之间　　交换路由信息　的协议。

边界网关协议　　BGP 只能是 力求寻找一条能够到达　　目的网络且　比较好 的路由（不能兜圈子），而 并非 要寻找一条 最佳 路由。

二十三、 IP 多播

1、 IP 多播的基本概念





2、 IP 多播的一些特点

(1) 多播使用组地址 —— IP 使用 D 类地址 支持多播。 多播地址 只能用于目的地址， 而不能用于源地址 。

(2) 永久组地址——由因特网号码指派管理局 IANA 负责指派。

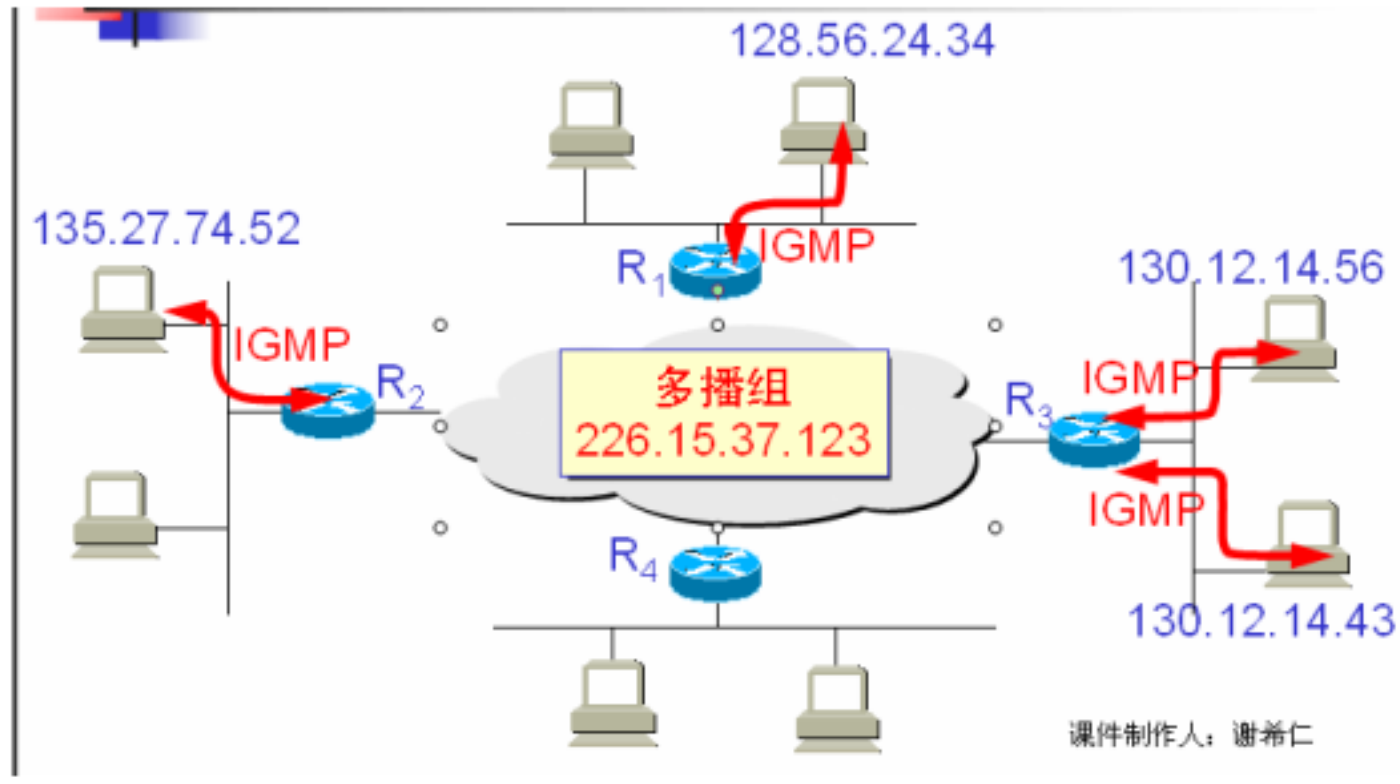
(3) 动态的组成员

(4) 使用硬件进行多播

3、 IP 多播需要两种协议

1）网际组管理协议 IGMP

为了使路由器 知道多播组成员的信息 ，需要利用 网际组管理协议 IGMP (Internet Group Management Protocol) 。



图示　IGMP　使多播路由器知道多播组成员信息

2）多播路由选择协议

连接在局域网上的多播路由器还必须和因特网上的其他多播路由器协同工作，以便　　把多播数据报用最小代价传送给所有的组成员　　。这就需要使用　多播路由选择协议　。

二十四、　专用地址（本地地址）和全球地址

本地地址　——仅在机构内部使用的　　IP　地址，可以由　本机构自行分配　，而 不需要 向因特网的管理机构　申请 。

全球地址　—— 全球唯一　的 IP 地址，　必须 向因特网的管理机构　　申请 。

2、专用地址（　**Private Address**）

10.0.0.0　到　10.255.255.255

172.16.0.0　到　172.31.255.255

192.168.0.0　到　192.168.255.255

这些地址只能用于一个机构的内部通信，而不能用于和因特网上的主机通信。

专用地址只能用作本地地址而不能用作全球地址。在因特网中的所有路由器对目的地址是专用地址的数据报一律不进行转发。

==========

第　**5**　章　　运输层

一　、应用进程之间的通信

两个主机进行通信实际上就是两个主机中的　　应用进程互相通信　。

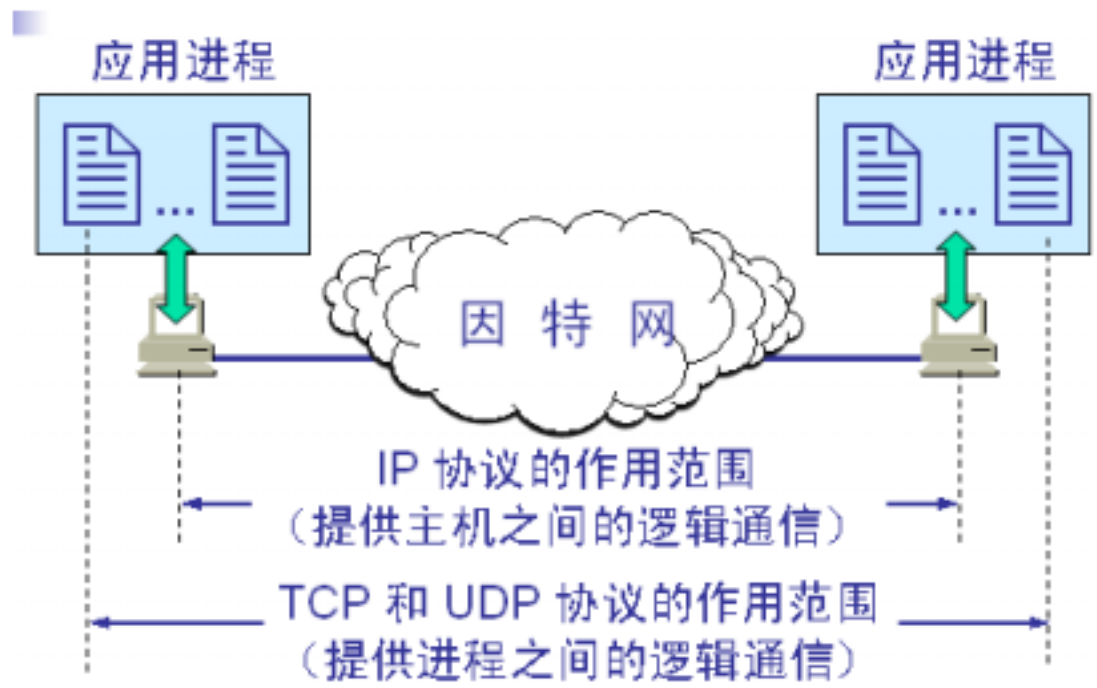
应用进程之间的通信又称为　　端到端的通信　。

运输层的一个很重要的功能就是　　复用 和 分用 。应用层不同进程的报文通过不同的端口向下交到运输层，再往下就共用网络层提供的服务。

“ 运输层提供应用进程间的逻辑通信 ”　　。“ 逻辑通信 ”的意思是：运输层之间的　　通信好像是沿水平方向传送数据　。但事实上这两个运输层之间并没有一条水平方向的物理连接。

二、运输层的主要功能

运输层为应用进程之间提供　　端到端的逻辑通信　（但网络层是为主机之间提供逻辑通信）　　。



图示　运输层协议和网络层协议的主要区别

运输层还要对收到的报文进行　　差错检测 。

运输层需要有两种不同的运输协议，即面向连接的　　TCP 和无连接的　UDP。

TCP 的特点：

TCP 是面向连接的运输层协议。

每一条　TCP 连接只能有两个端点 (endpoint)，每一条　TCP 连接只能是点对点的（　一对一 ）。

TCP 提供可靠交付的服务。

TCP 提供全双工通信。

面向 字节流 。

注意：

TCP 连接是一条 虚连接 而不是一条真正的物理连接。

TCP 对应用进程一次把多长的报文发送到　　TCP 的缓存中是不关心的。

TCP 根据对方给出的窗口值和当前网络拥塞的程度来决定一个报文段应包含多少个字节　　（UDP 发送的报文长度是应用进程给出的）。

TCP 可把太长的数据块划分短一些再传送。　　TCP 也可等待积累有足够多的字节后再构成报文段发送出去。

UDP 是面向报文的 ：

发送方 UDP 对应用程序交下来的报文，在添加首部后就向下交付 IP 层。 UDP 对应用层交 下来的报文，既不合并，也不拆分，而是保留这些报文的边界。

应用层交给 UDP 多长的报文， UDP 就照样发送，即一次发送一个报文。

接收方 UDP 对 IP 层交上来的 UDP 用户数据报，在去除首部后就原封不动地交付上层的应用进程，一次交付一个完整的报文。

应用程序必须选择合适大小的报文。

三、 TCP 的端口

端口用一个 16 位端口号进行标志。

端口号只具有 本地 意义，即端口号只是为了标志本计算机应用层中的各进程。在因特网中不同计算机的相同端口号是没有联系的。

四、 TCP 的连接

TCP 把连接作为最基本的抽象。

每一条 TCP 连接有 两个端点 。

TCP 连接的端点不是主机， 不是主机的 IP 地址， 不是应用进程， 也不是运输层的协议端口。 TCP 连接的端点叫做 套接字 (socket)或插口。

端口号拼接到 (contatenated with) IP 地址即构成了套接字。

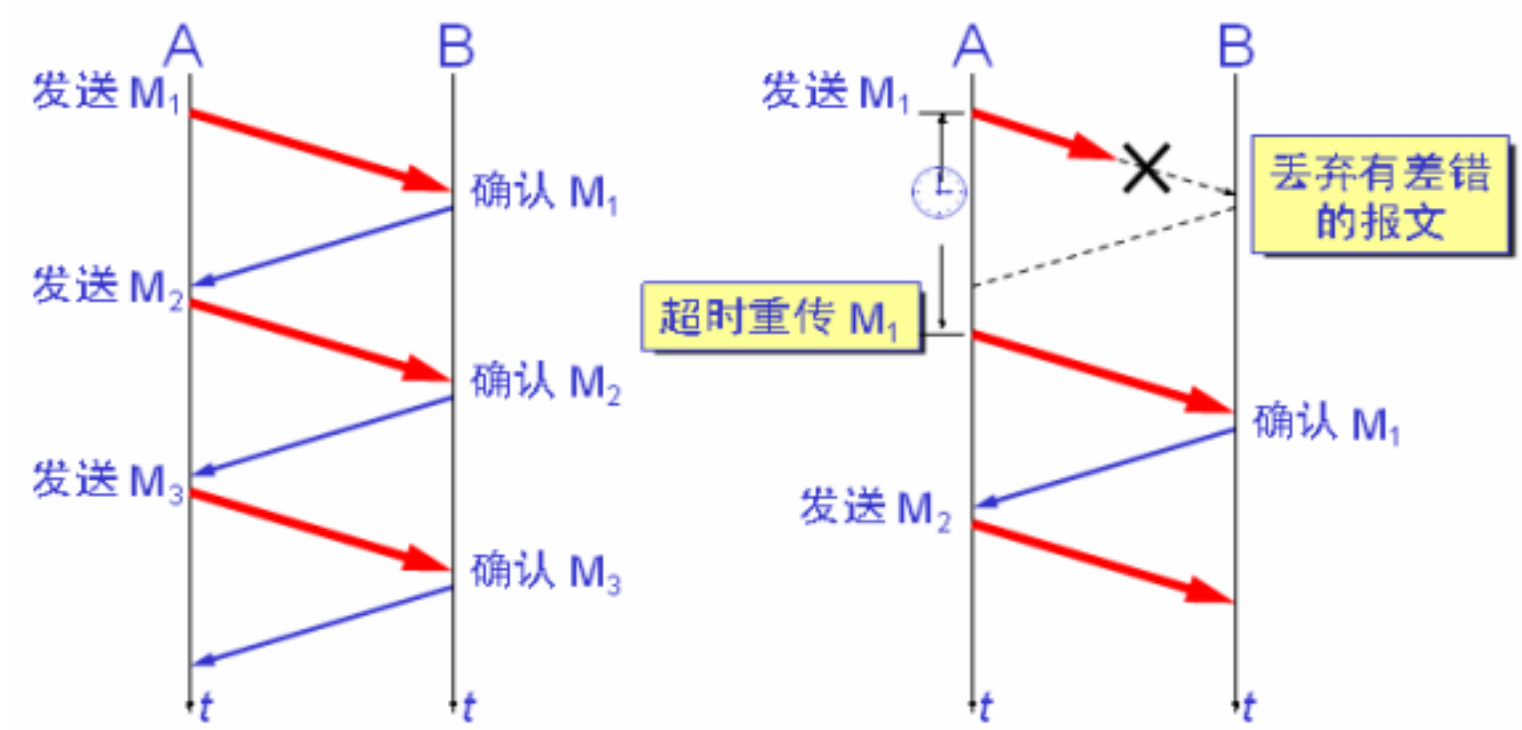
套接字 socket = (IP 地址 : 端口号)

每一条 TCP 连接唯一地被通信两端的两个端点（即两个套接字）所确定。即：

TCP 连接 ::= {socket1, socket2} = {(IP1: port1), (IP2: port2)}

五、可靠传输的工作原理

1、停止等待协议



(a) 无差错情况　　(b) 超时重传

请注意：

1)　在发送完一个分组后，必须　暂时保留 已发送的分组的　副本。

2)　分组和确认分组都必须进行编号。

3)　超时计时器的重传时间应当比数据在分组传输的平均往返时间更长一些。

可靠通信的实现　：

使用上述的 确认和重传机制，我们就可以 在不可靠的传输网络上实现可靠的通信。

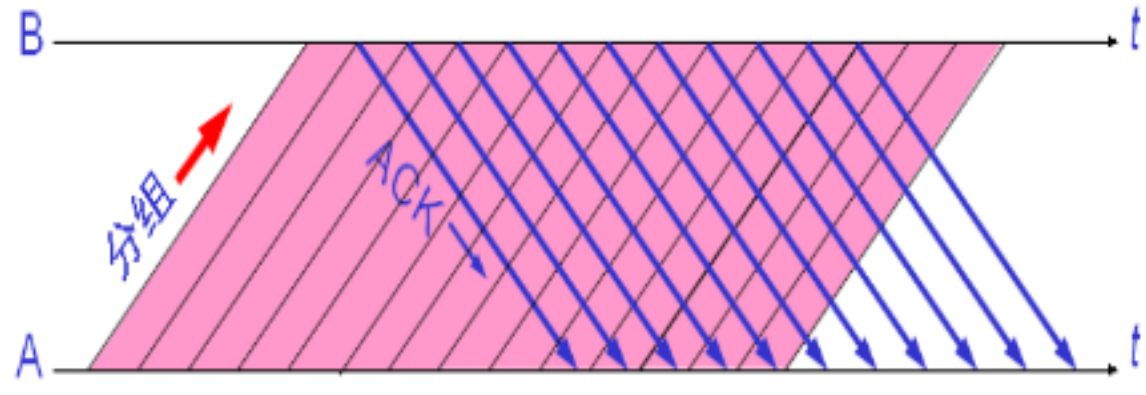
这种可靠传输协议常称为自动重传请求　　ARQ (Automatic Repeat reQuest) 。

ARQ 表明重传的请求是自动进行的。接收方不需要请求发送方重传某个出错的分组　　。

2、流水线传输

发送方可连续发送多个分组，不必每发完一个分组就停顿下来等待对方的确认。

由于信道上一直有数据不间断地传送，这种传输方式可获得很高的信道利用率。



六、 **TCP** 的流量控制——利用　滑动窗口 实现

流量控制 (flow control) 就是让发送方的发送速率不要太快，既要让接收方来得及接收，也不要使网络发生拥塞。

利用滑动窗口机制可以很方便地在　　TCP 连接上实现流量控制。

七、　**TCP** 的运输连接管理

1、运输连接的三个阶段

运输连接就有三个阶段，即： 连接建立 、 数据传送 和 连接释放 。运输连接的管理就是使运输连接的 建立和释放都能正常地进行。

连接建立过程中要解决以下三个问题：

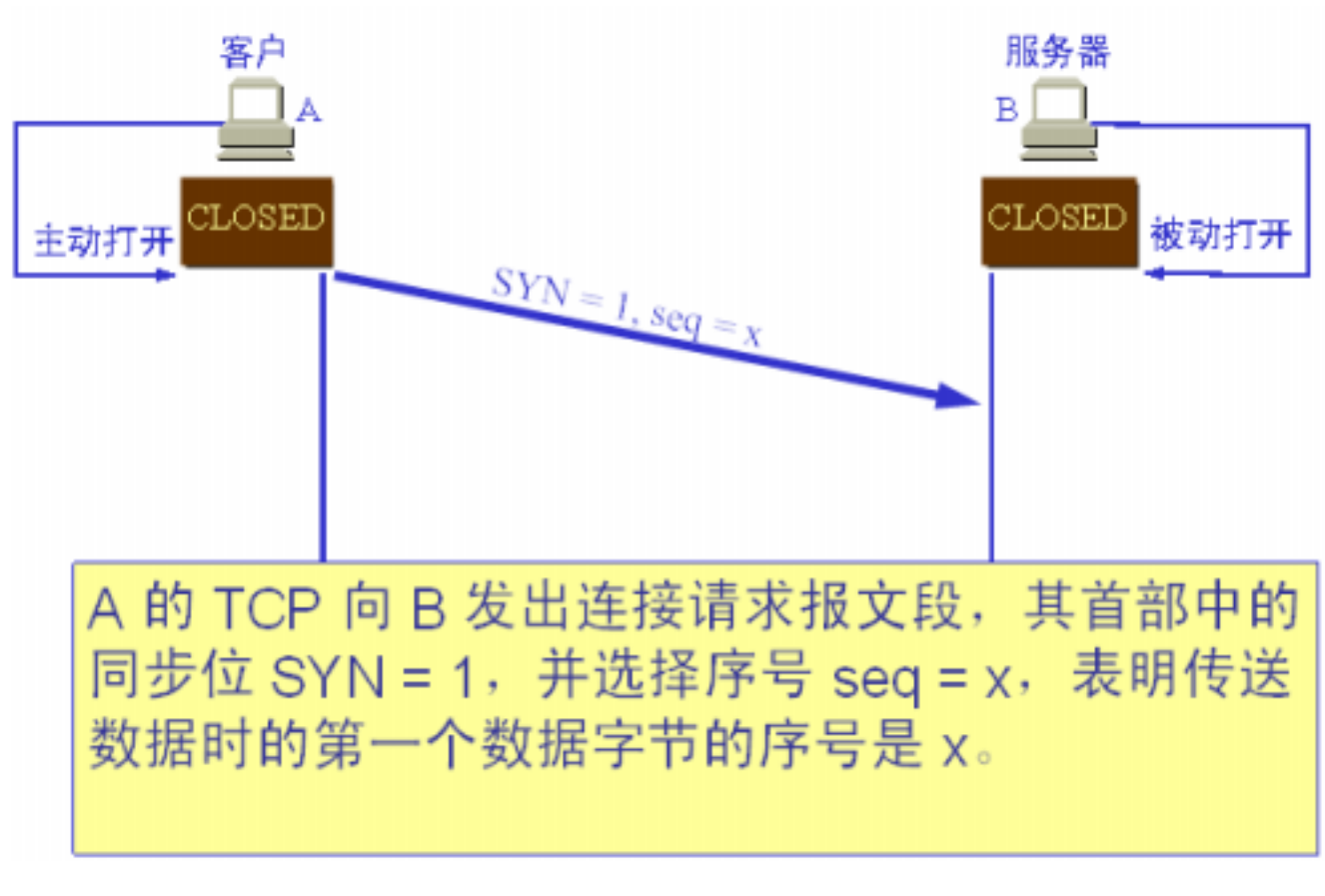
要使每一方能够确知对方的存在。

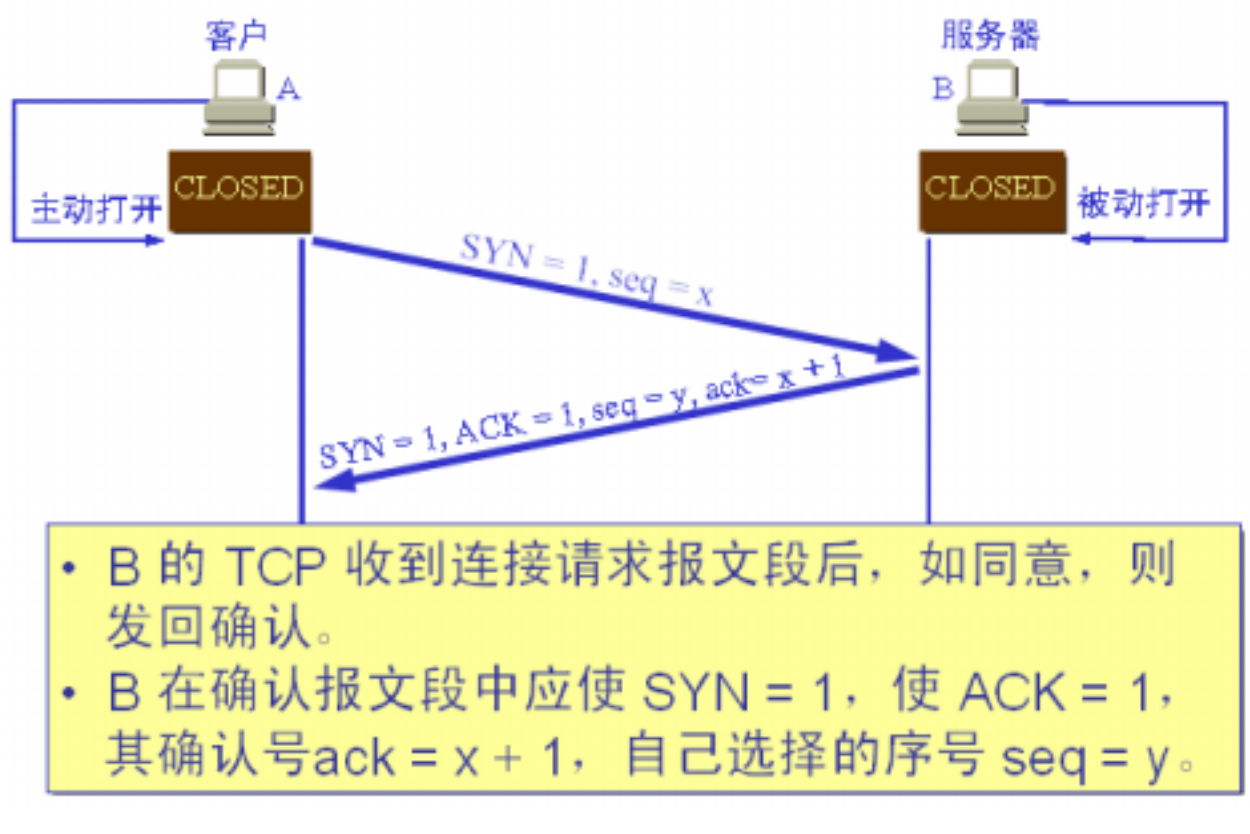
要允许双方协商一些参数（如最大报文段长度，最大窗口大小，服务质量等） 。

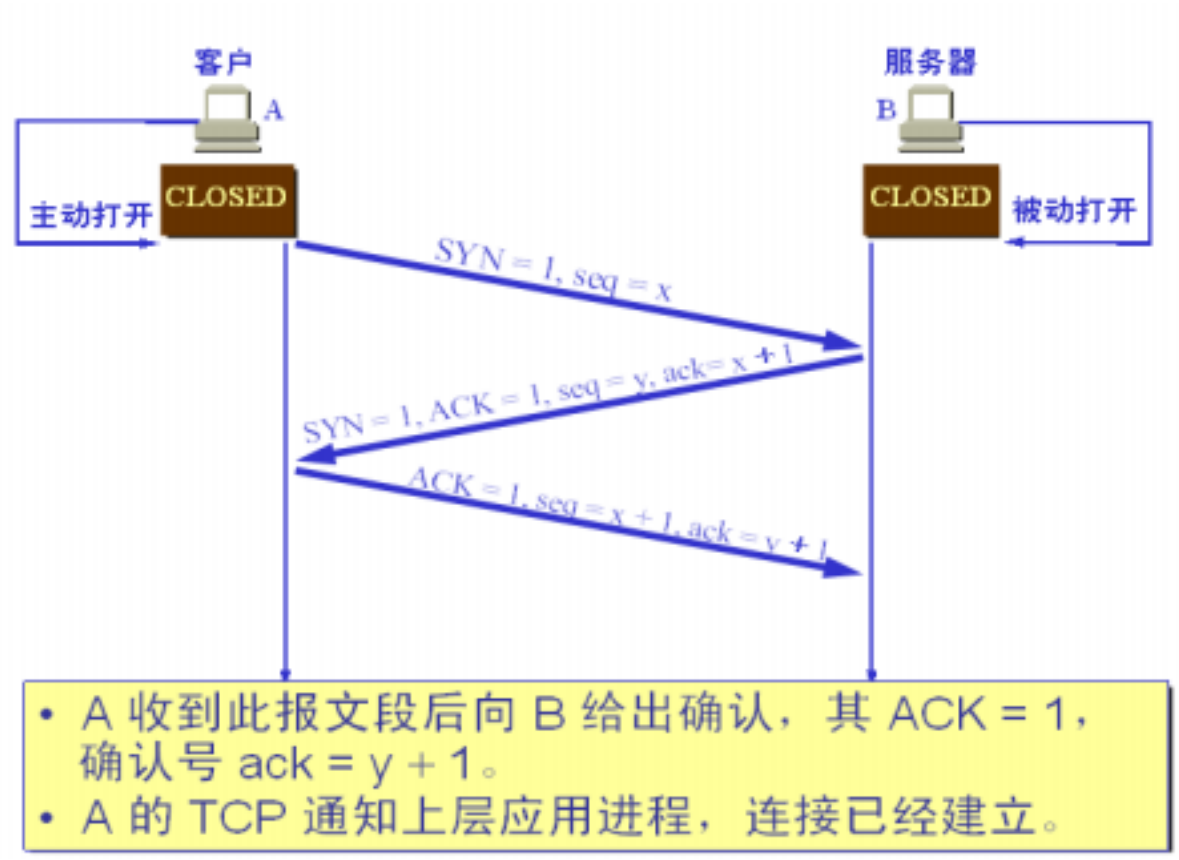
能够对运输实体资源（如缓存大小，连接表中的项目等）进行分配。

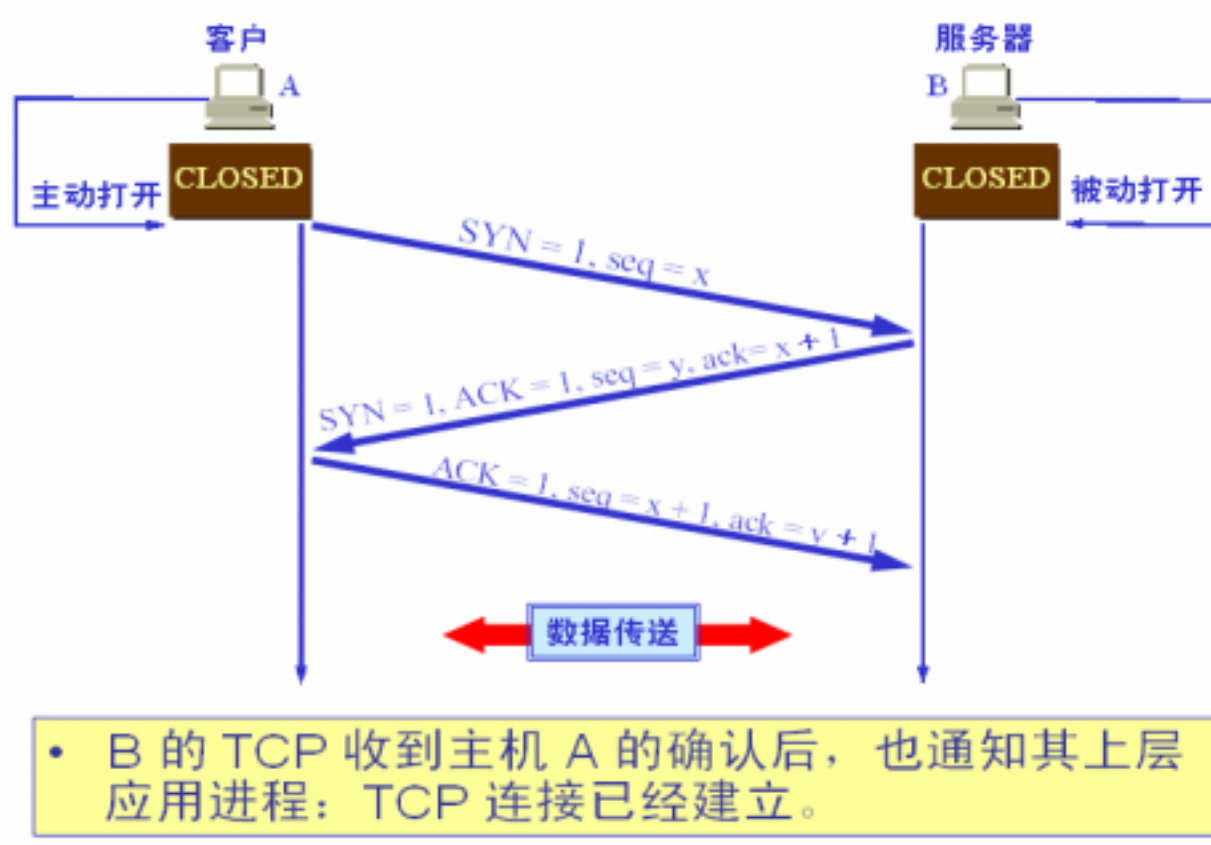
TCP 连接的建立都是采用客户服务器方式。

2.TCP 的连接建立——用三次握手建立 **TCP** 链接

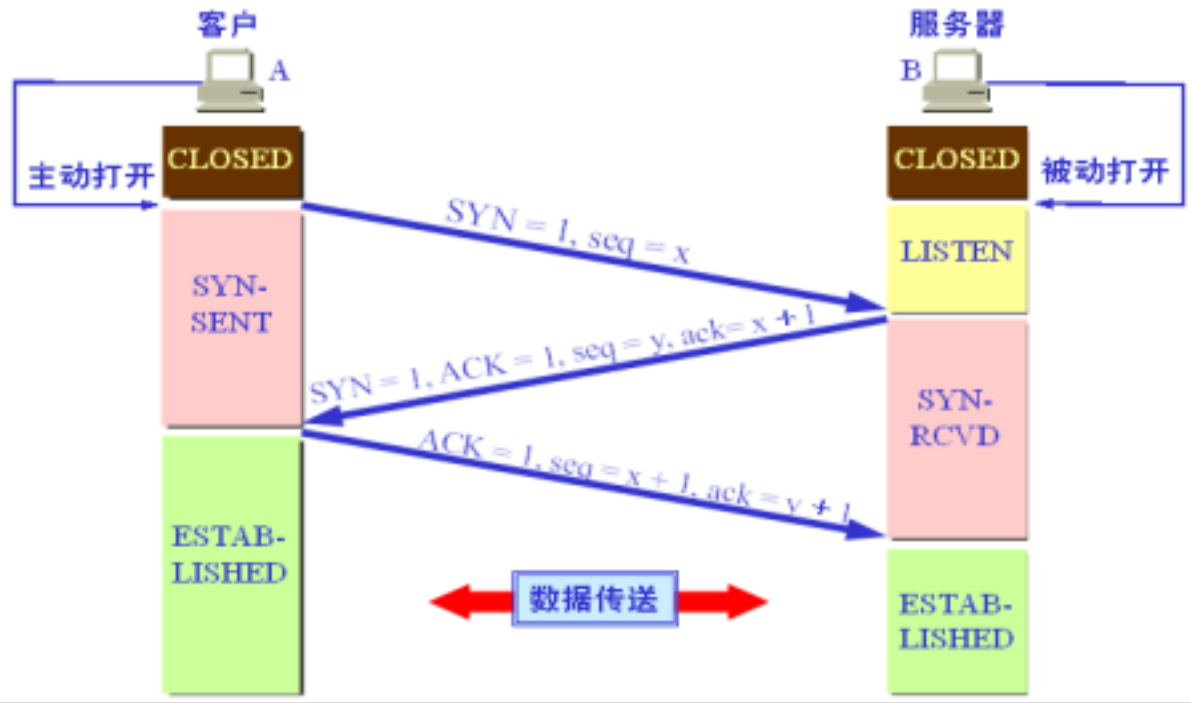








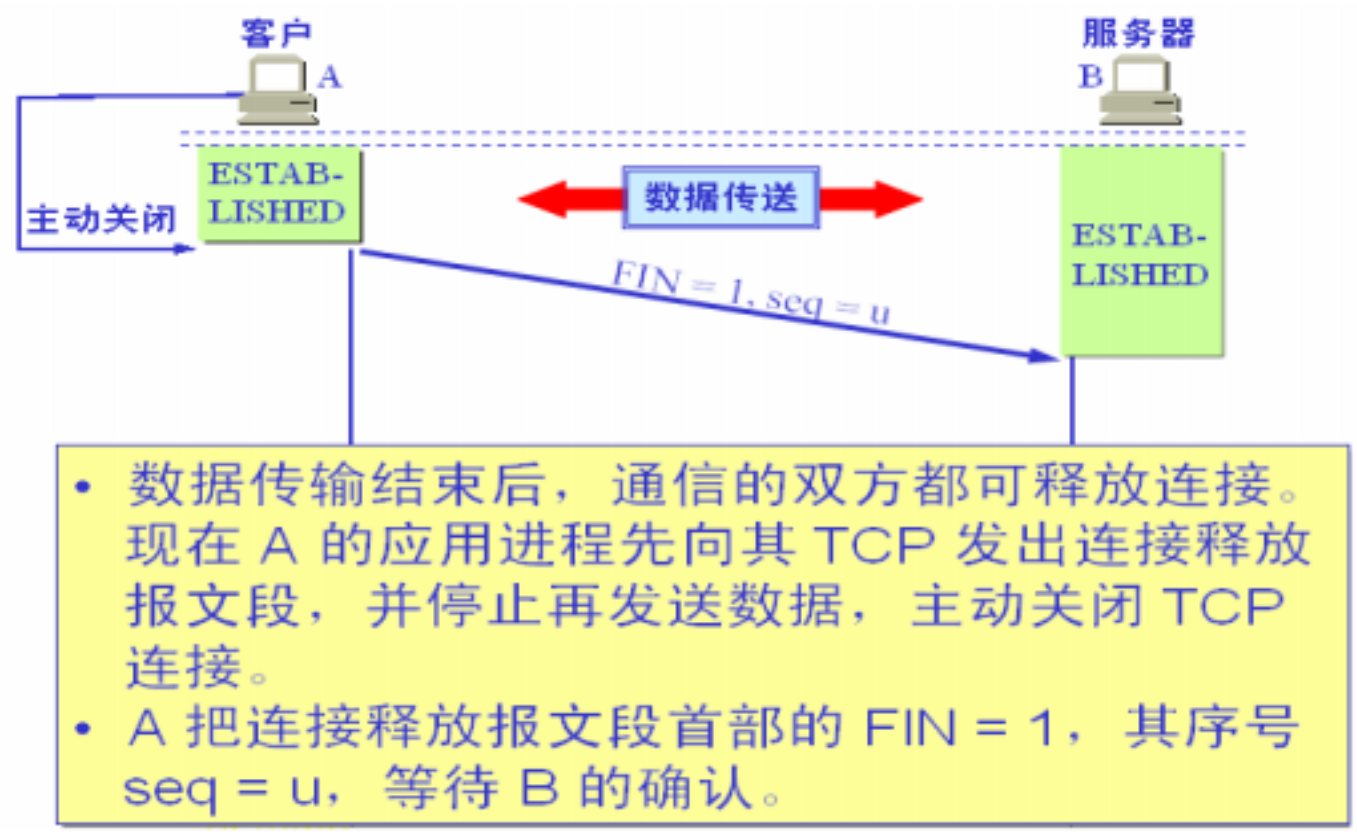
3、用三次握手建立 **TCP** 连接的各状态 ：



4、连接的释放

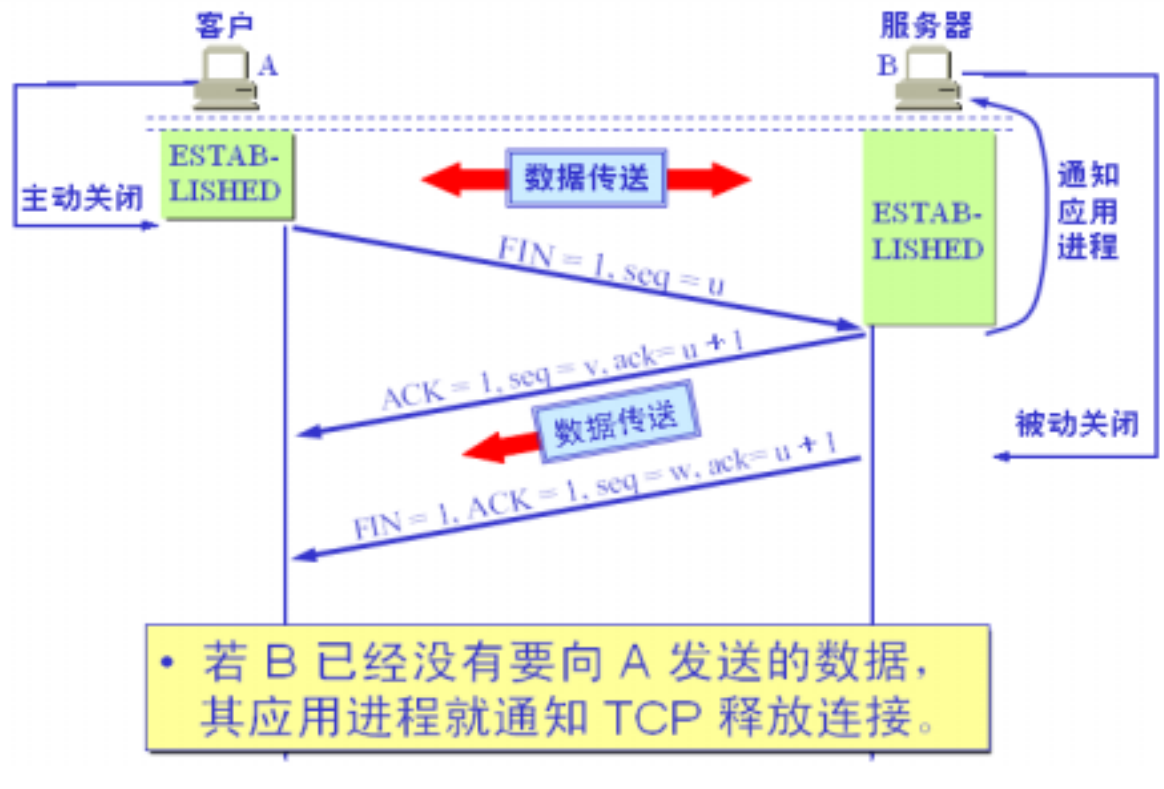
数据传输结束后，双方都可释放连接，但一方 (设为 A) 释放连接前需获得另一方 (设为 B) 的允许，如果此时 B 方仍有数据要传输， 则连接不得释放， A 仍要接收 B 的数据， 直至 B 方数据传输完毕后， B 方发出释放连接的要求，得到 A 方的许可确认后， B 释放连接， A 等待 2SML 后释放连接，此时通信结束。

如下图所示：

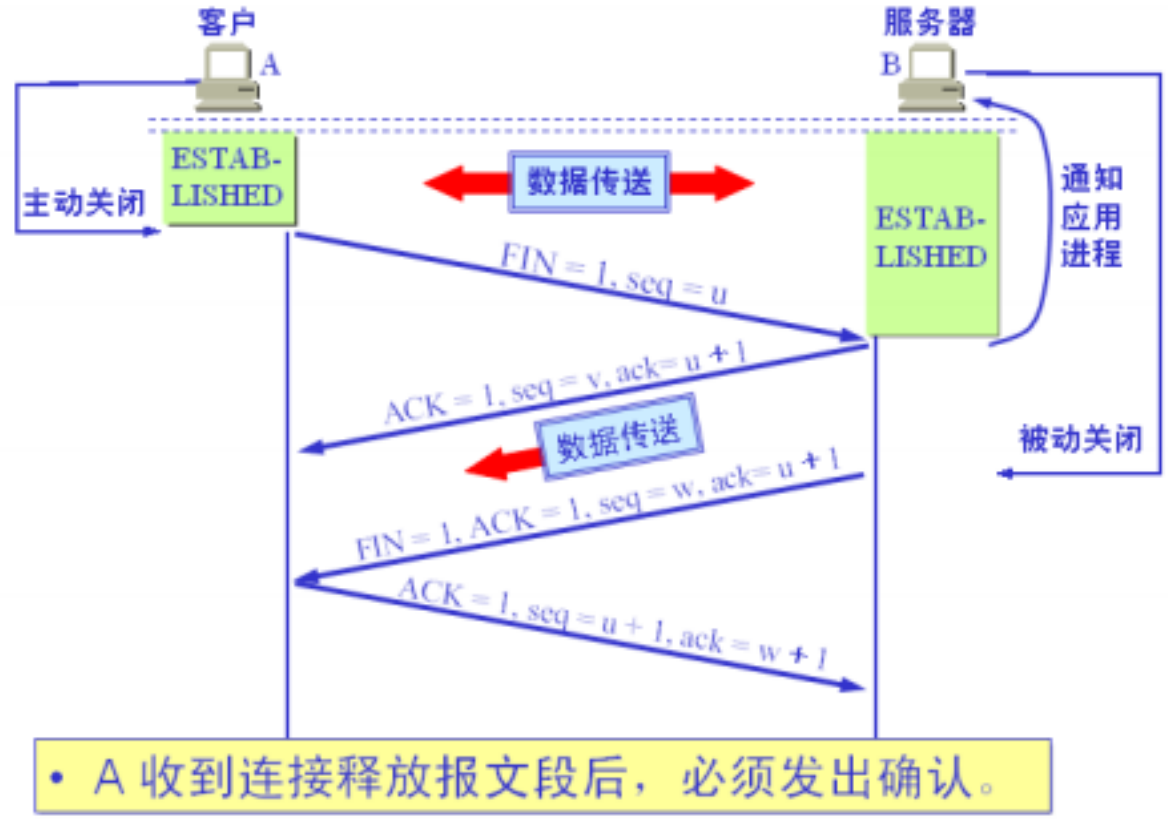


- 数据传输结束后，通信的双方都可释放连接。现在 A 的应用进程先向其 TCP 发出连接释放报文段，并停止再发送数据，主动关闭 TCP 连接。
- A 把连接释放报文段首部的 FIN = 1，其序号 seq = u，等待 B 的确认。

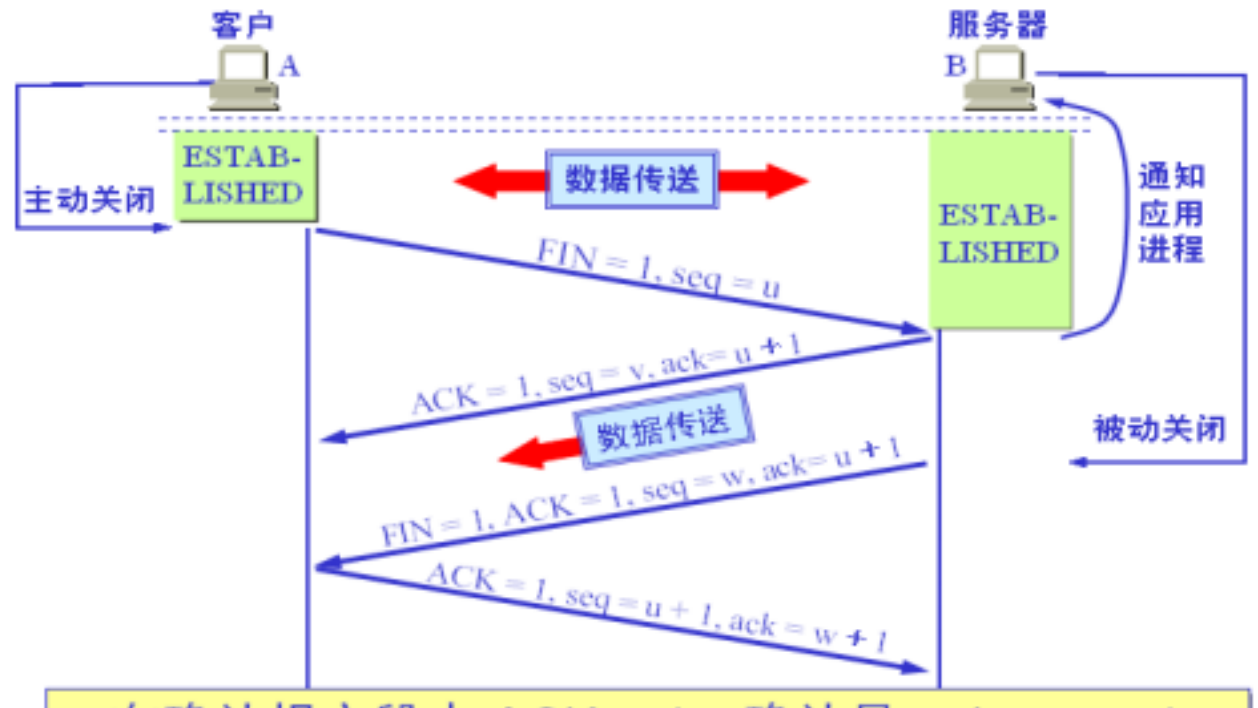
- B 发出确认，确认号 ack = u + 1，而这个报文段自己的序号 seq = v。
- TCP 服务器进程通知高层应用进程。
- 从 A 到 B 这个方向的连接就释放了，TCP 连接处于半关闭状态。B 若发送数据，A 仍要接收。



- 若 B 已经没有要向 A 发送的数据，其应用进程就通知 TCP 释放连接。

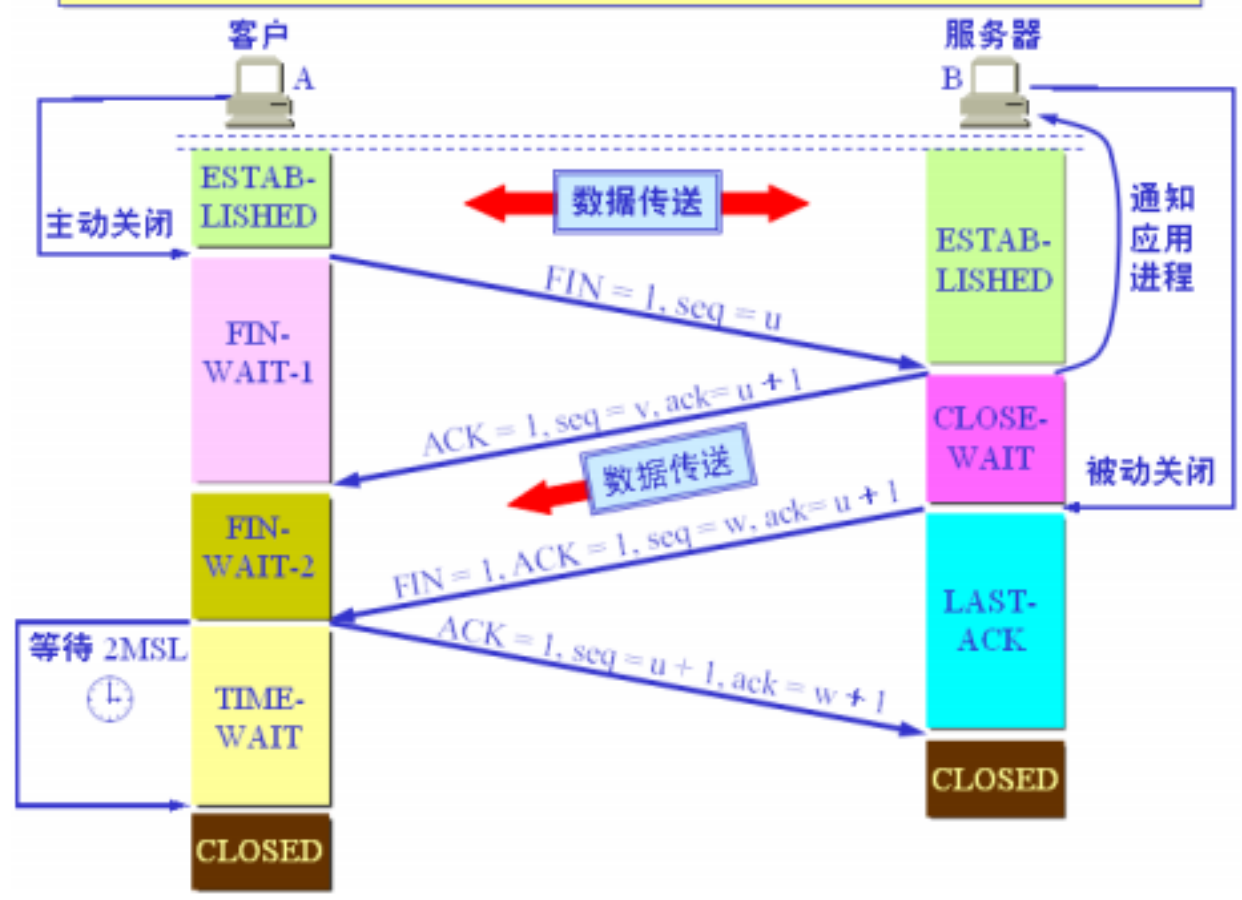


• A 收到连接释放报文段后，必须发出确认。



• 在确认报文段中 ACK = 1，确认号 ack = w + 1，
自己的序号 seq = u + 1。

TCP 连接必须经过时间 2MSL 后才真正释放掉。



==========

第六章　应用层

一、应用层协议的特点

每个应用层协议都是为了解决某一类应用问题，而问题的解决又往往是通过位于不同主机中的多个应用进程之间的通信和协同工作来完成的。应用层的具体内容就是　　规定应用进程在通信时所遵循的协议 。

应用层的许多协议都是基于　客户服务器方式　。

二、域名系统　**DNS**

计算机的用户只是间接而不是直接使用域名系统。

因特网采用 层次结构的命名树　作为主机的名字，并使用　分布式的域名系统　DNS。

名字到　IP 地址的解析是由　若干个域名服务器程序　完成的。域名服务器程序在专设的结点上运行，运　行该程序的机器称为域名服务器。

三、层次树状结构的命名方法

任何一个连接在因特网上的主机或路由器，都有一个　　唯一 的层次结构的名字，即　域名 。

域名的结构由标号序列组成，各标号之间用点隔开：

，　．三级域名　．二级域名　．顶级域名

各标号分别代表不同级别的域名。

四、域名只是个逻辑概念

域名只是个逻辑概念，并不代表计算机所在的物理地点。

变长的域名和使用有助记忆的字符串，是为了便于人来使用。而　　IP 地址是定长的　32 位二进制数字则非常便于机器进行处理。

域名中的“ 点 ”和点分十进制　　IP 地址中的“ 点 ”并无一一对应的关系　　。点分十进制　IP 地址中一定是包含三个“ 点 ”　，但每一个域名中“ 点 ”的数目则不一定正好是三个。

五、顶级域名　**TLD(Top Level Domain)**

(1) 国家顶级域名　**nTLD** ：如：.cn 表示中国，　.us 表示美国，　.uk 表示英国，等等。

(2) 通用顶级域名　**gTLD** ：最早的顶级域名是：

.com　（公司和企业）　　.net　（网络服务机构）

.org　（非赢利性组织）　　.edu　（美国专用的教育机构（）

.gov （美国专用的政府部门） .mil （美国专用的军事部门）

.int （国际组织）

(3) 基础结构域名 **(infrastructure domain)** ：这种顶级域名只有一个，即 arpa，用于反向域名解析，因此又称为反向域名。

六、域名服务器的四种类型

根 域名服务器

根域名服务器是最重要的域名服务器。所有的根域名服务器都知道所有的顶级域名服务器的域名和 IP 地址。

不管是哪一个本地域名服务器， 若要对因特网上任何一个域名进行解析， 只要自己无法解析，就首先求助于根域名服务器。

在因特网上共有 13 个不同 IP 地址的根域名服务器（注意这里的 13 是指共有 13 套装置，而不是 13 个机器），它们的名字是用一个英文字母命名，从 a 一直到 m（前 13 个字母）。这些根域名服务器相应的域名分别是

a.rootservers.net

b.rootservers.net

，

m.rootservers.net

到 2006 年底全世界已经安装了 一百多个 根域名服务器 机器，分布在世界各地。

顶级 域名服务器

这些域名服务器负责管理在该顶级域名服务器注册的所有二级域名。

当收到 DNS 查询请求时，就给出相应的回答（可能是最后的结果，也可能是下一步应当找的域名服务器的 IP 地址）。

权限 域名服务器

这就是前面已经讲过的 负责一个区 的域名服务器。

当一个权限域名服务器还不能给出最后的查询回答时，就会告诉发出查询请求的 DNS 客户，下一步应当找哪一个权限域名服务器。

本地 域名服务器

本地域名服务器对域名系统非常重要。

当一个主机发出 DNS 查询请求时，这个查询请求报文就发送给本地域名服务器。

每一个因特网服务提供者 ISP，或一个大学，甚至一个大学里的系，都可以拥有一个本地域名服务器，

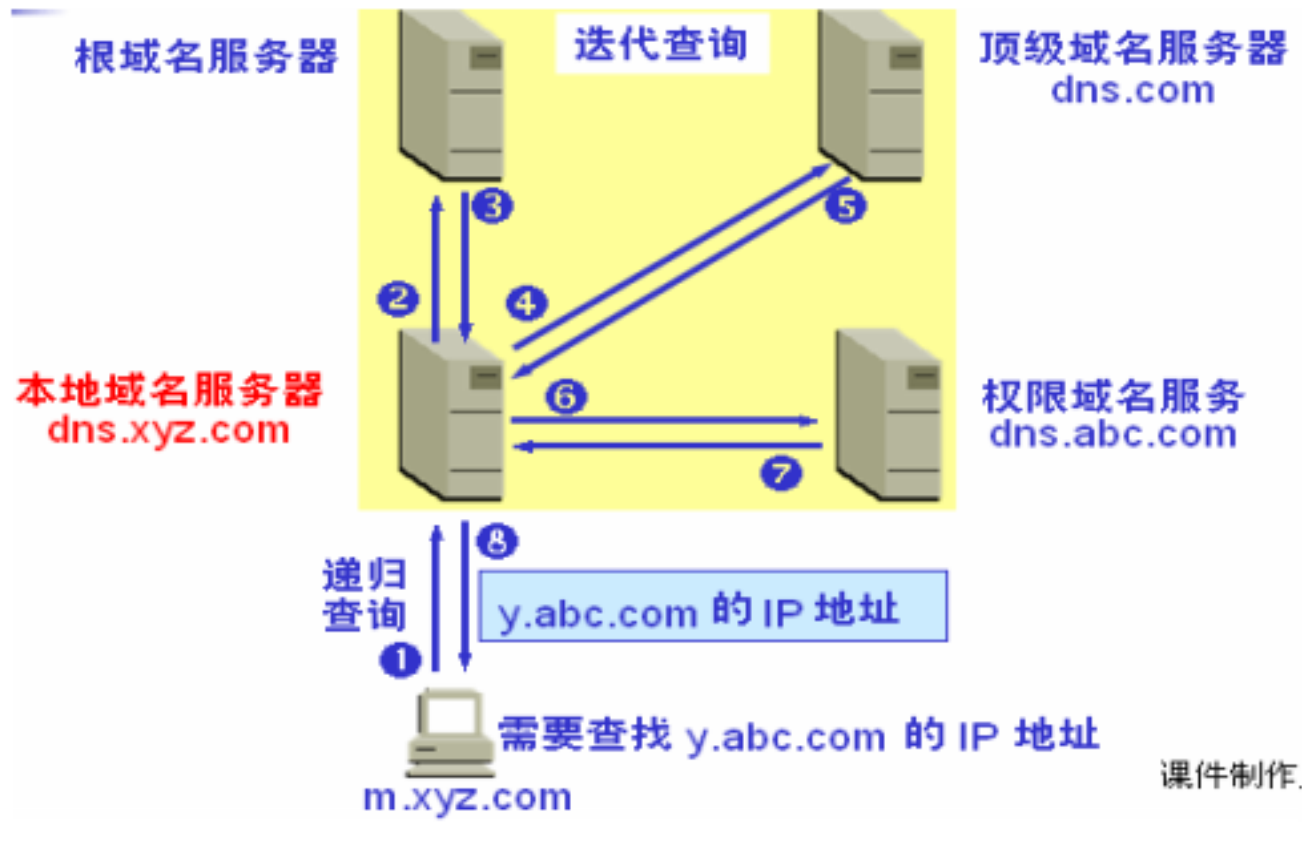
这种域名服务器有时也称为 默认域名服务器 。

七、域名的解析过程

主机向本地域名服务器　的查询一般都是采用　递归查询 。如果主机所询问的本地域名服务器不知道被查询域名的　IP 地址，那么本地域名服务器就以　　DNS 客户的身份，向其他根域名服务器继续发出查询请求报文。

本地域名服务器向根域名服务器　　的查询通常是采用　迭代查询 。当根域名服务器收到本地域名服务器的迭代查询请求报文时，　要么给出所要查询的　　IP 地址，要么告诉本地域名服务器：　“ 你下一步应当向哪一个域名服务器进行查询 ”　。然后让本地域名服务器进行后续的查询。

以上两种方式如下图所示：



八、文件传送协议

1、 FTP (File Transfer Protocol)　概述

FTP 是因特网上使用得最广泛的文件传送协议。

FTP 提供交互式的访问，允许客户指明文件的类型与格式，并允许文件具有存取权限。

FTP 屏蔽了各计算机系统的细节　　，因而 适合于在异构网络　中任意计算机之间传送文件。

九、文件传送并非很简单的问题

1．网络环境中的一项基本应用就是将文件从一台计算机中复制到另一台可能相距很远的计算机中。

2．初看起来，在两个主机之间传送文件是很简单的事情。

3．其实这往往非常困难。原因是众多的计算机厂商研制出的　　文件系统多达数百种，且差别很大　　。

十、网络环境下复制文件的复杂性：

(1) 计算机存储数据的格式不同。

(2) 文件的目录结构和文件命名的规定不同。

(3) 对于相同的文件存取功能，操作系统使用的命令不同。

(4) 访问控制方法不同。

十一、 FTP 特点

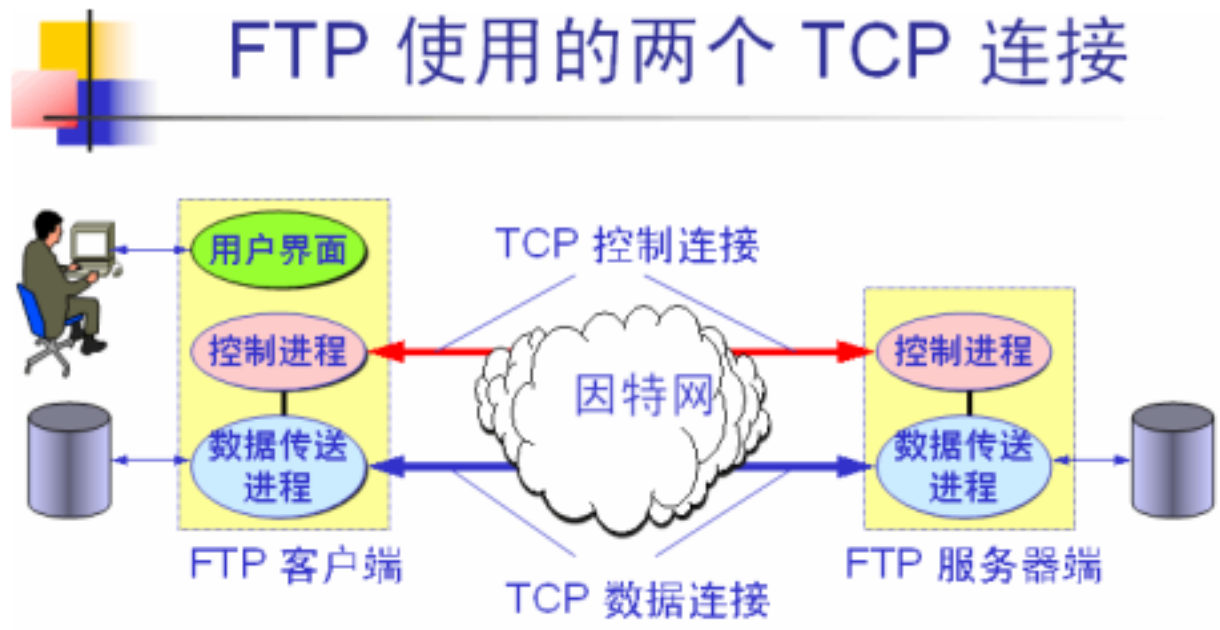
文件传送协议 FTP 只提供文件传送的一些基本的服务，它使用 TCP 可靠的运输服务。

FTP 的主要功能是 减少或消除在不同操作系统下处理文件的不兼容性 。

FTP 使用客户服务器方式。一个 FTP 服务器进程可同时为多个客户进程提供服务。 FTP 的服务器进程由两大部分组成： 一个主进程 ，负责接受新的请求；另外有 若干个从属进程 ，负责处理单个请求。

两个连接

控制连接 在整个会话期间一直保持打开， FTP 客户发出的传送请求通过控制连接发送给服务器端



的控制进程，但控制连接不用来传送文件。

实际用于传输文件的是 “ 数据连接 ”。服务器端的控制进程在接收到 FTP 客户发送来的文件传输请求后就创建“ 数据传送进程 ”和“ 数据连接 ” ，用来连接客户端和服务器端的数据传送进程。

数据传送进程实际完成文件的传送，在传送完毕后关闭“ 数据传送连接 ”并结束运行。

两个不同的端口号

当客户进程向服务器进程发出建立连接请求时，要寻找连接服务器进程的 熟知端口 (21)，同时还要告诉服务器进程自己的另一个端口号码，用于建立数据传送连接。

接着，服务器进程用自己传送数据的 熟知端口 (20)与客户进程所提供的端口号码建立数据传送连接。

由于 FTP 使用了两个不同的端口号，所以数据连接与控制连接不会发生混乱。 20 号端口

21 号端口

十二、简单文件传送协议　**TFTP(Trivial File Transfer Protocol)**

TFTP 是一个很小且易于实现的文件传送协议。

TFTP 使用客户服务器方式和　使用　UDP 数据报，因此　TFTP 需要有自己的差错改正措施。

TFTP 只支持文件传输而不支持交互。

TFTP 没有一个庞大的命令集，没有列目录功能，也不能对用户进行身份鉴别。

十三、万维网的文档

HTML　文档是一种可以用　任何文本编辑器　创建的　ASCII　码 文件。

万维网的文档可以分为以下　　3 类：

静态文档 是指该文档创作完毕后就存放在万维网服务器中，在被用户浏览的过程中，内容不会改变。

动态文档 是指文档的内容是在浏览器访问万维网服务器时才由应用程序动态创建。

动态文档和静态文档之间的主要差别体现在　　服务器一端　。这主要是文档内容的　生成方法不同　。而从浏览器的角度看，这两种文档并没有区别。

活动万维网文档　(可以用　Java 技术创建活动文档　)

活动文档 (active document) 技术把所有的工作都转移给浏览器端。

每当浏览器请求一个活动文档时，服务器就返回一段程序副本在浏览器端运行。

Java 技术装三个主要组成部分：程序设计语言、运行　　**(runtime)** 环境（ **JVM** ）和　类库。

十四、两种不同的链接

远程链接：超链的终点是其他网点上的页面。

本地链接：超链指向本计算机中的某个文件。

十五、通用网关接口　**CGI(Common Gateway Interface)**

CGI 是一种标准，它定义了　动态文档应如何创建　，输入 数据应如何提供给应用程序　，以及 输出结果应如何使用　。

万维网服务器与　CGI 的通信遵循　CGI 标准。

“ 通用 ”：CGI 标准所定义的规则对其他任何语言都是通用的。

“ 网关 ”：CGI 程序的作用像网关。

“ 接口 ”：有一些已定义好的变量和调用等可供其他　　CGI 程序使用。

十六、 万维网的信息检索系统

在万维网中用来进行搜索的程序叫做 搜索引擎。

全文检索搜索引擎 是一种纯技术型的检索工具。它的工作原理是通过搜索软件到因特网上的各网站收集信息，找到一个网站后可以从这个网站再链接到另一个网站。然后按照一定的规则建立一个很大的在线数据库供用户查询。

用户在查询时只要输入关键词，就从已经建立的索引数据库上进行查询（并不是实时地在因特网上检索到的信息） 。

分类目录搜索引擎（ 分类网站搜索 ）并不采集网站的任何信息，而是利用各网站向搜索引擎提交的网站信息时填写的关键词和网站描述等信息， 经过人工审核编辑后， 如果认为符合网站登录的条件，则输入到分类目录的数据库中，供网上用户查询。

垂直搜索引擎 (Vertical Search Engine) 针对某一特定领域、特定人群或某一特定需求提供搜索服务。垂直搜索也是提供关键字来进行搜索的，但被放到了一个行业知识的上下文中，返回的结果更倾向于信息、消息、条目等。

十七、电子邮件

发送邮件的协议： SMTP

读取邮件的协议： POP3 和 IMAP

MIME 在其邮件首部中说明了邮件的 数据类型 (如文本、声音、图像、视像等)，使用 MIME 可在邮件中同时传送多种类型的数据。

电子邮件的最主要的组成构件： 用户代理 、发送端邮件服务器 、接收端邮件服务器 。

用户代理 UA 就是用户与电子邮件系统的接口，是电子邮件客户端软件。

十八、简单邮件传送协议 **SMTP**

SMTP 所规定的就是在两个相互通信的 SMTP 进程之间应如何交换信息。

由于 SMTP 使用客户服务器方式，因此负责发送邮件的 SMTP 进程就是 SMTP 客户 ，而负责接收邮件的 SMTP 进程就是 SMTP 服务器 。

SMTP 规定了 14 条命令和 21 种应答信息。每条命令用 4 个字母组成，而每一种应答信息一般只有一行信息，由一个 3 位数字的代码开始，后面附上（也可不附上）很简单的文字说明。

十九、 **SMTP** 通信的三个阶段

连接建立、邮件传送、连接释放。

二十、邮件读取协议 POP3 和 IMAP

邮局协议 POP（Post Office Protocol ） 是一个非常简单、但功能有限的邮件读取协议，现在使用的是它的第三个版本 POP3。

POP 也使用 客户服务器 的工作方式。

在接收邮件的用户 PC 机中必须运行 POP 客户程序，而在用户所连接的 ISP 的邮件服务器中则运行 POP 服务器程序。

因特网 报文 存取协议 IMAP （Internet Message Access Protocol）也是按 客户服务器 方式工作， 现在较新的是版本 4，即 IMAP4 。

用户在自己的 PC 机上就可以操纵 ISP（Internet Service Provider ） 的邮件服务器的邮箱，就像在本地操纵一样。

因此 IMAP 是一个联机协议。当用户 PC 机上的 IMAP 客户程序打开 IMAP 服务器的邮箱时，用户就可看到邮件的首部。若用户需要打开某个邮件，则该邮件才传到用户的计算机上。

IMAP 的特点

允许收件人只读取邮件中的某一个部分。

二十一、发送和接收电子邮件的几个重要步骤

1) 发件人调用 PC 机中的用户代理撰写和编辑要发送的邮件。

2) 发件人的用户代理把邮件用 SMTP 协议发给发送方邮件服务器，

3) SMTP 服务器把邮件临时存放在 邮件缓存队列 中，等待发送。

4) 发送方邮件服务器的 SMTP 客户与接收方邮件服务器的 SMTP 服务器建立 TCP 连接，然后就把 邮件缓存队列 中的邮件 依次发送 出去。

5) 运行在接收方邮件服务器中的 SMTP 服务器进 程收到邮件后，把邮件放入收件人的用户邮箱中，等待收件人进行读取。

6) 收件人在打算收信时，就运行 PC 机中的用户代理，使用 POP3（或 IMAP ）协议读取发送给自己的邮件。

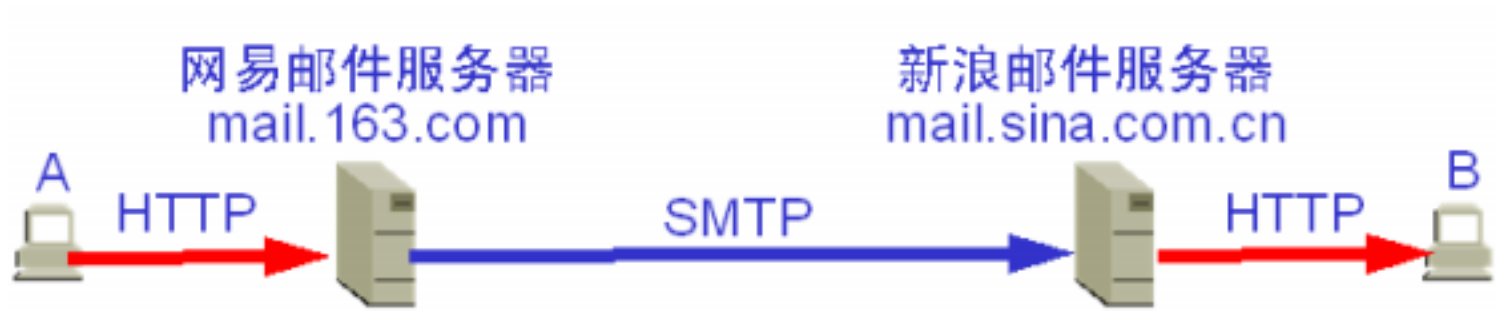
7) 请注意 ， POP3 服务器和 POP3 客户之间的通信是由 POP3 客户发起的。

二十二、基于万维网的电子邮件

电子邮件从 A 发送到网易邮件服务器是使用 HTTP 协议。

两个邮件服务器之间的传送使用 SMTP。

邮件从新浪邮件服务器传送到 B 是使用 HTTP 协议。



二十三、通用因特网邮件扩充　　**MIME**

SMTP　有以下缺点：

1)　SMTP　不能传送可执行文件或其他的二进制对象。

2)　SMTP　限于传送　7 位的　ASCII　码。许多其他非英语国家的文字（如中文、俄文，甚至带重音符号的法文或德文）就无法传送。

3)　SMTP　服务器会拒绝超过一定长度的邮件。

4)　某些　SMTP　的实现并没有完全按照　[RFC 821] 的　SMTP　标准。

MIME　的特点：

MIME　并没有改动　SMTP　或取代它。

MIME　的意图是继续使用目前的　[RFC 822] 格式，但　增加了邮件主体的结构　，并定义了传送　非　ASCII 码的编码规则　。

MIME　和　SMTP　的关系

MIME　主要包括三个部分　：

1)　5　个新的邮件首部字段　，这些字段提供了有关邮件主体的信息。

①　MIME-Version:　标志　MIME　的版本。现在的版本号是　　1.0。若无此行，则为英文文本。

②　Content-Description:　这是可读字符串，说明此邮件是什么。和邮件的主题差不多。

③　Content-Id:　邮件的唯一标识符。

④　Content-Transfer-Encoding：在传送时邮件的主体是如何编码的。

⑤　Content-Type：说明邮件的性质。

2)　定义了许多　邮件内容的格式　，对多媒体电子邮件的表示方法进行了标准化。

MIME　的标准规定　Content-Type　说明必须含有两个标识符，即内容类型　　(type) 和子类型

(subtype)，中间用“ / ”分开，如 text/html ， text/css 等。

MIME 标准定义了 7 个基本内容类型和 15 种子类型。

3) 定义了 传送编码 ，可对任何内容格式进行转换，而不会被邮件系统改变。

① 最简单的编码就是 7 位 ASCII 码，而每行不能超过 1000 个字符。 MIME 对这种由 ASCII 码构成的邮件主体不进行任何转换。

② 另一种编码称为 quoted-printable ，这种编码方法适用于当所传送的数据中只有少量的非 ASCII 码。

③ 对于任意的二进制文件，可用 base64 编码。

二十四、动态主机配置协议 DHCP(Dynamic Host Configuration Protocol)

动态主机配置协议 DHCP 提供了 即插即用连网 (plug-and-play networking) 的机制。

这种机制允许一台计算机加入新的网络和获取 IP 地址而不用手工参与。

DHCP 使用客户服务器方式：

需要 IP 地址的主机在启动时就向 DHCP 服务器广播发送 发现报文 （DHCP DISCOVER ），这时该主机就成为 DHCP 客户。

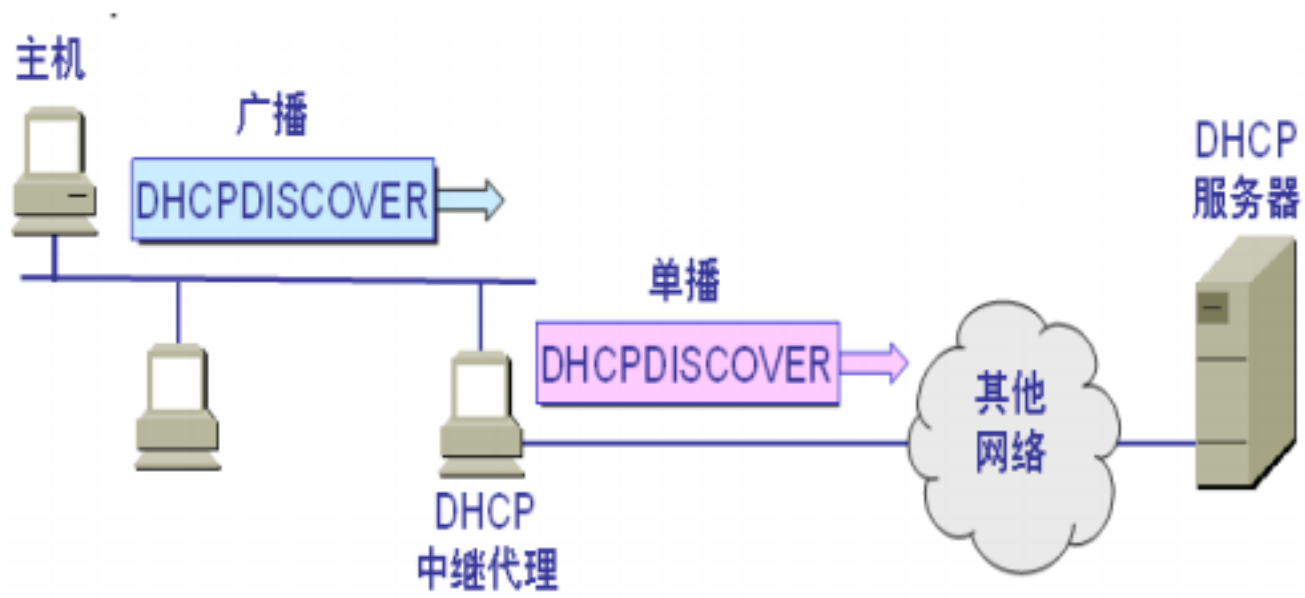
本地网络上所有主机都能收到此广播报文，但只有 DHCP 服务器才回答此广播报文。

DHCP 服务器先在其数据库中查找该计算机的配置信息。若找到，则返回找到的信息。若找不到，则从服务器的 IP 地址池 (address pool)中取一个地址分配给该计算机。 DHCP 服务器的回答报文叫做 提供报文 （DHCP OFFER）。

DHCP 中继代理（ relay agency）

并不是每个网络上都有 DHCP 服务器，这样会使 DHCP 服务器的数量太多。 现在是每一个网络至少有一个 DHCP 中继代理 ，它配置了 DHCP 服务器的 IP 地址信息。

当 DHCP 中继代理收到主机发送的发现报文后， 就以单播方式向 DHCP 服务器转发此报文， 并等待其回答。收到 DHCP 服务器回答的提供报文后， DHCP 中继代理再将此提供报文发回给主机。



租用期 (lease period)

DHCP 服务器分配给 DHCP 客户的 IP 地址的临时的， 因此 DHCP 客户只能在一段有限的时间

内使　　用这个分配到的　　IP 地址。 DHCP 协议称这段时间为　租用期 。

租用期的数值应由　　DHCP 服务器自己决定。

DHCP 客户也可在自己发送的报文中（例如，发现报文）提出对租用期的要求。

二十五、简单网络管理协议　　SNMP

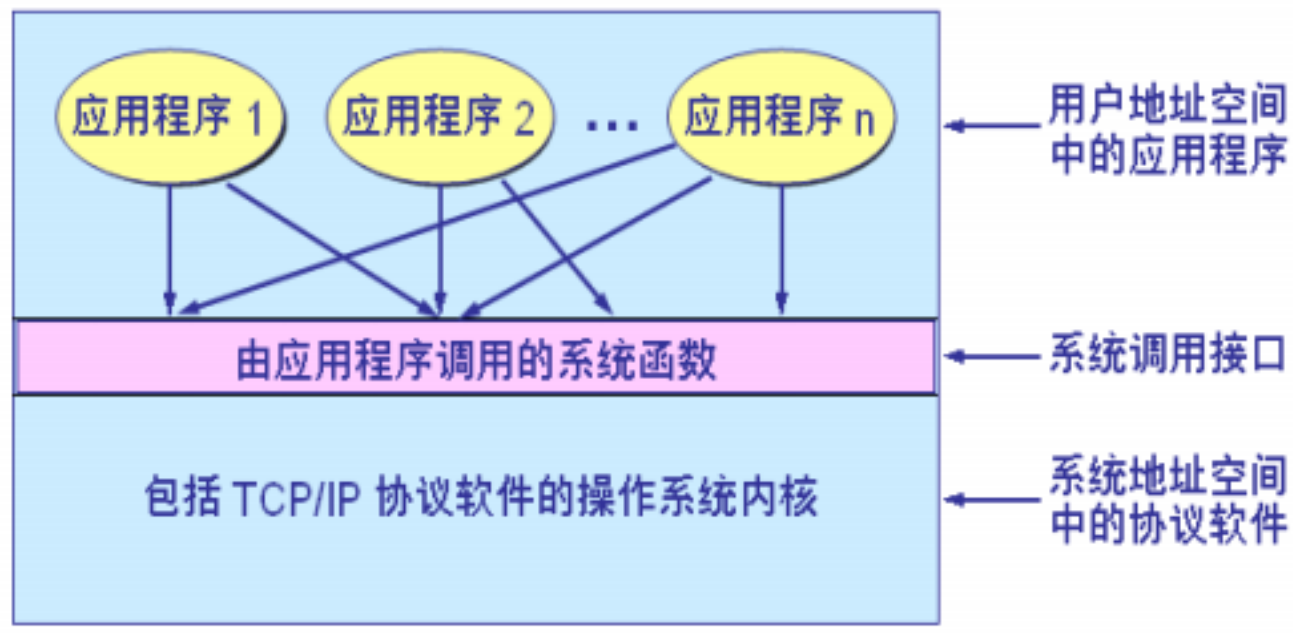
SNMP 使用无连接的　UDP

二十六、应用进程跨越网络的通信

1、系统调用

大多数操作系统使用　系统调用 (system call)的机制在 应用程序和操作系统　之间 传递控制权 。

对程序员来说，每一个系统调用和一般程序设计中的　　函数调用 非常相似，只是系统调用是将控制权传递给了操作系统。



多个应用进程使用系统调用的机制

2、应用编程接口　**API(Application Programming Interface)**

当某个应用进程启动系统调用时，控制权就从应用进程传递给了　　系统调用接口 。

此接口再将控制权传递给计算机的操作系统。操作系统将此调用转给某个内部过程，并执行所请求的操作。

内部过程一旦执行完毕，控制权就又通过系统调用接口返回给应用进程。

系统调用接口实际上就是应用进程的控制权和操作系统的控制权进行转换的一个接口，即　　应用编程接口　API。

2.1 几种应用编程接口　　API

①　Berkeley UNIX　操作系统定义了一种　　API，它又称为 套接字接口 (socket interface)。

②　微软公司在其操作系统中采用了套接字接口　　API，形成了一个稍有不同的　　API，并称之为 Windows Socket。

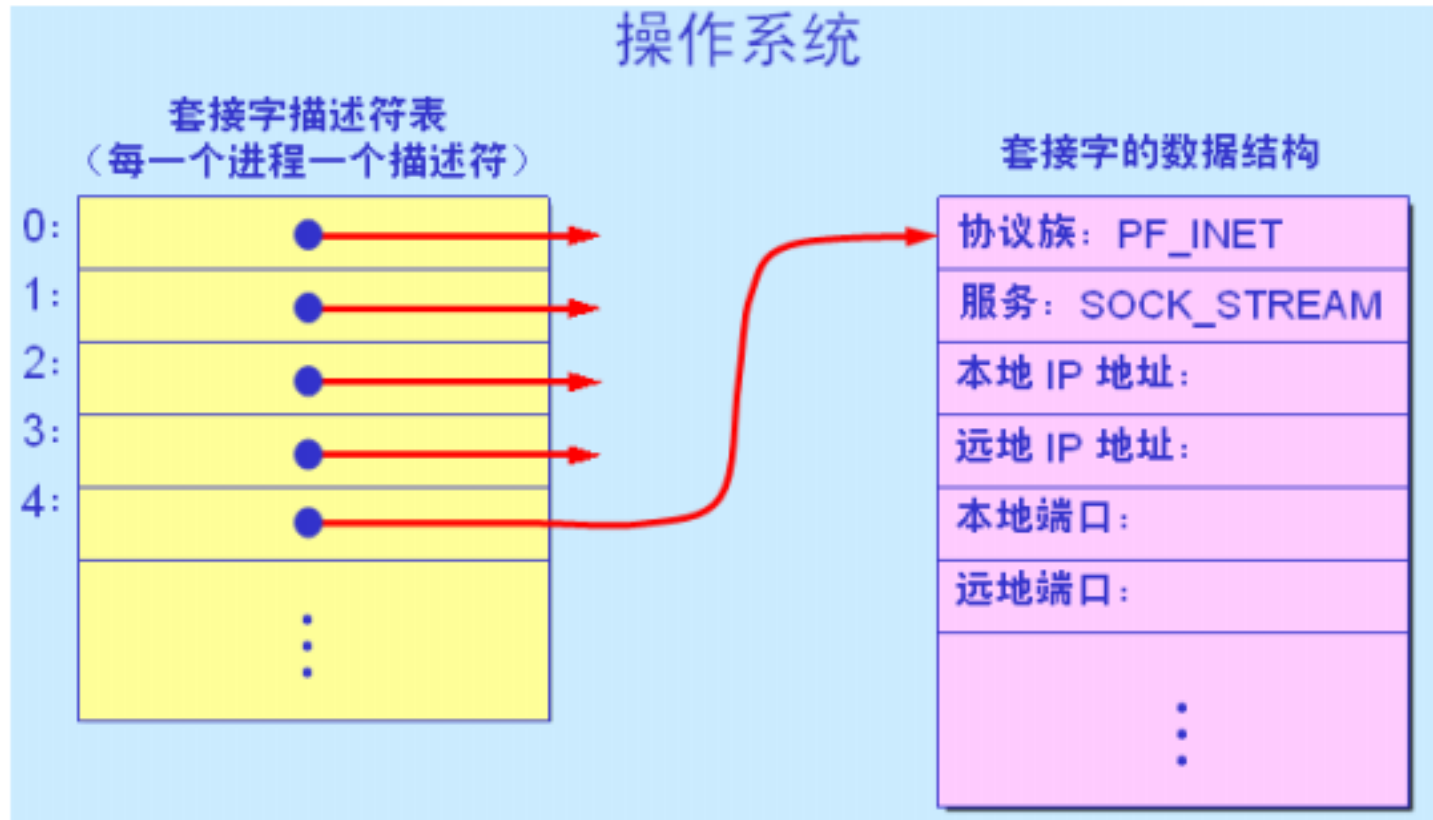
③　AT&T 为其 UNIX 系统 V 定义了一种　API，简写为　TLI (Transport Layer Interface) 。

2.1.1 套接字的作用

当应用进程需要使用网络进行通信时就发出系统调用，请求操作系统为其创建“套接字”，以便把网络通信所需要的系统资源分配给该应用进程。

操作系统为这些资源的总和用一个叫做套接字描述符的号码来表示，并把此号码返回给应用进程。应用进程所进行的网络操作都必须使用这个号码。

通信完毕后，应用进程通过一个关闭套接字的系统调用通知操作系统回收与该“号码”相关的所有资源。



调用 socket 创建套接字

==========

第七章 网络安全

一、计算机网络面临的安全性威胁

计算机网络上的通信面临以下的四种威胁：

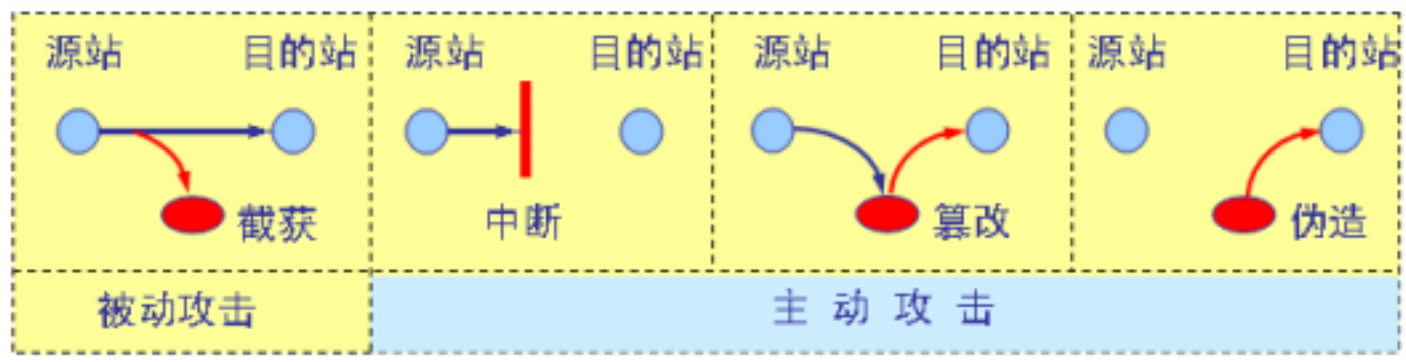
(1) 截获——从网络上窃听他人的通信内容。

(2) 中断——有意中断他人在网络上的通信。

(3) 篡改——故意篡改网络上传送的报文。

(4) 伪造——伪造信息在网络上传送。

截获信息的攻击称为被动攻击，而更改信息和拒绝用户使用资源的攻击称为主动攻击。



二、被动攻击和主动攻击

被动攻击 ——攻击者只是 观察和分析 某一个 协议数据单元 PDU 而不干扰信息流。

主动攻击 —— 是指攻击者对某个连接中通过的 PDU 进行各种处理，如：

更改 报文流

拒绝 报文 服务

伪造 连接初始化

三、计算机网络通信安全的目标

(1) 防止析出报文内容；

(2) 防止通信量分析；

(3) 检测更改报文流；

(4) 检测拒绝报文服务；

(5) 检测伪造初始化连接。

四、恶意程序 **(rogue program)**

(1) 计算机病毒 ——会“传染”其他程序的程序，“传染”是通过修改其他程序来把自身或其变种 复制进去完成的。

(2) 计算机蠕虫 ——通过网络的通信功能将自身从一个结点 发送 到另一个结点 并启动运行 的程序。

(3) 特洛伊木马 ——一种程序，它执行的功能超出所声称的功能。

(4) 逻辑炸弹 ——一种当运行环境满足某种特定条件时执行其他特殊功能的程序。

五、计算机网络安全的内容

保密性

安全协议的设计

访问控制

六、公钥密码体制

公钥密码体制使用不同的加密密钥与解密密钥，是一种“　　由已知加密密钥推导出解密密钥在计算上是不可行的　”密码体制。

1、公钥和私钥

在公钥密码体制中，　加密密钥（即公钥）PK（Public Key）　是公开信息，而　解密密钥（即私钥或秘钥　）SK(Secret Key)　是需要保密的。

加密算法　E(Encrypt)　和解密算法　D　也都是公开的。

虽然秘钥　SK　是由公钥　PK　决定的，但却不能根据　　PK　计算出　SK。

2、公钥算法的特点

发送者　A　用　B　的公钥　PKB　对明文　X　加密（E　运算）后，在接收者　B　用自己的私钥　SKB　解密（D　运算），即可恢复出明文：

$$D_{SK_B}(Y) = D_{SK_B}(E_{PK_B}(X)) = X$$

解密密钥是接收者专用的秘钥，对其他人都保密。

加密密钥是公开的，但不能用它来解密　　，即

$$D_{PK_B}(E_{PK_B}(X)) \neq X$$

加密和解密的运算可以对调，即

$$E_{PK_B}(D_{SK_B}(X)) = D_{SK_B}(E_{PK_B}(X)) = X$$

在计算机上可容易地产生成对的　　PK　和　SK。

从已知的　PK　实际上不可能推导出　　SK，即从　PK　到　SK　是“计算上不可能的　”。

加密和解密算法都是公开的　　。

七、　数字签名

数字签名必须保证以下三点：

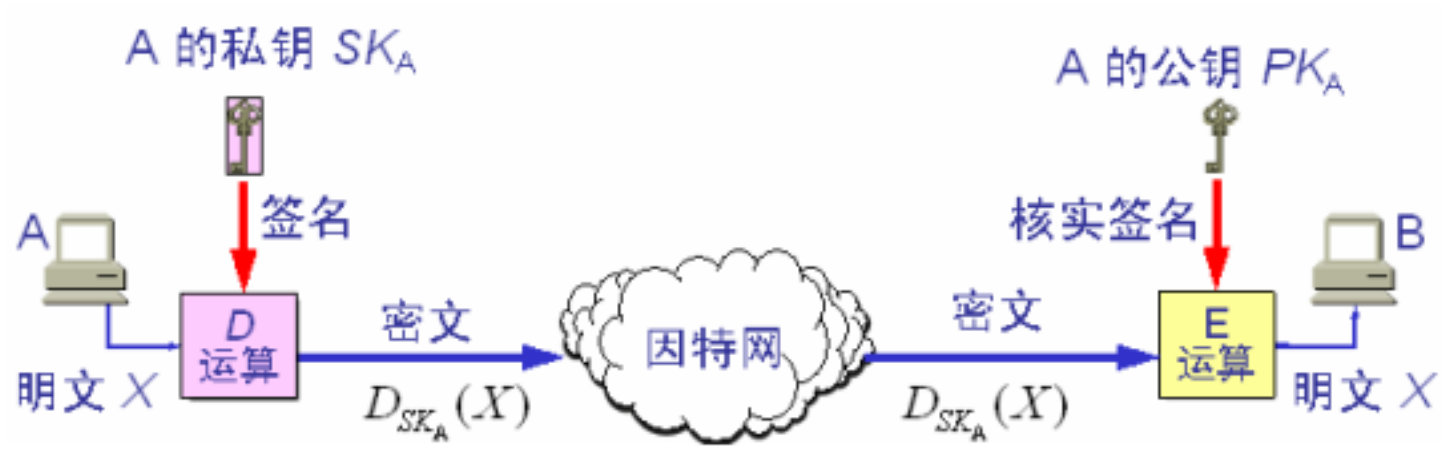
(1)　报文鉴别　——接收者能够核实发送者对报文的签名；

(2)　报文的完整性　——发送者事后不能抵赖对报文的签名；

(3)　不可否认　——接收者不能伪造对报文的签名。

现在已有多种实现各种数字签名的方法。但采用　　公钥算法　更容易实现。

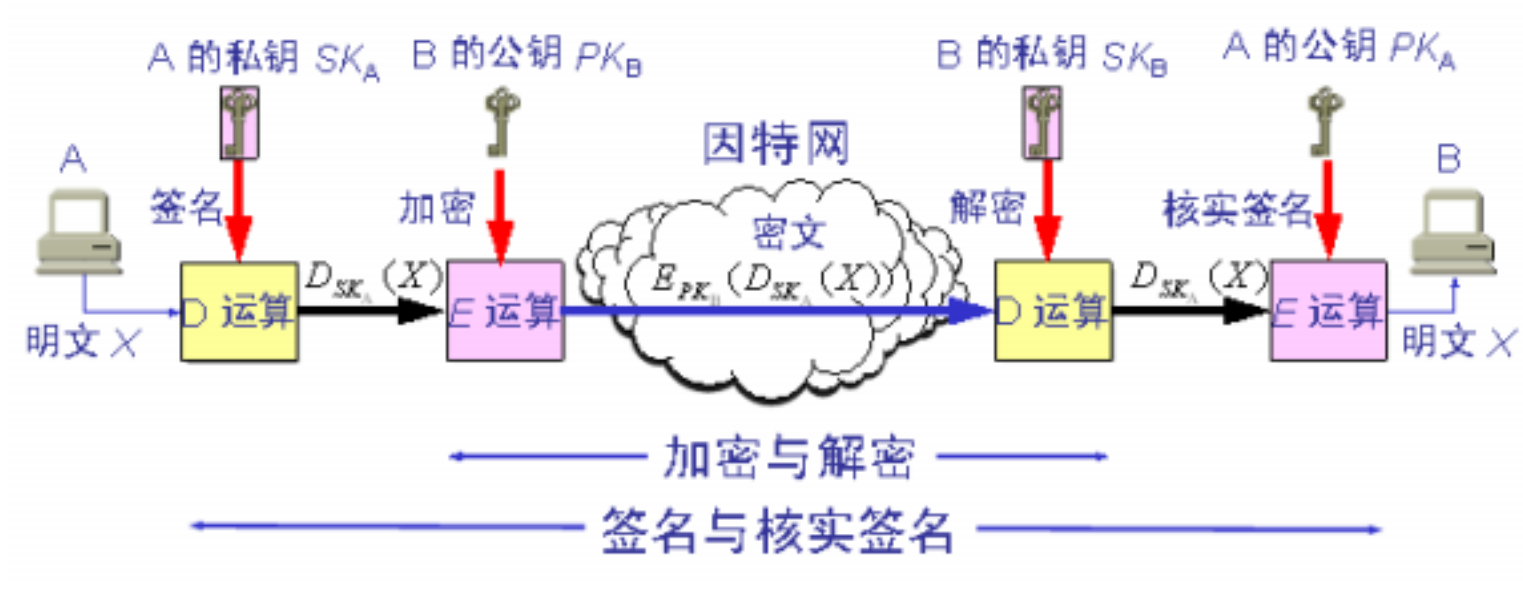
数字签名的实现　　：



因为除 A 外没有别人能具有 A 的私钥，所以除 A 外没有别人能产生这个密文。 因此 B 相信报文 X 是 A 签名发送的。

若 A 要抵赖曾发送报文给 B，B 可将明文和对应的密文出示给第三者。 第三者很容易用 A 的公钥去证实 A 确实发送 X 给 B。

反之，若 B 将 X 伪造成 X‘，则 B 不能在第三者前出示对应的密文。 这样就证明了 B 伪造了报文。



具有保密性的数字签名

八、鉴别

在信息的安全领域中， 对付被动攻击 的重要措施是 加密，而 对付主动攻击 中的篡改和伪造则要用 鉴别 (authentication) 。

报文鉴别使得通信的接收方能够验证所收到的报文 （发送者和报文内容、 发送时间、 序列等） 的真伪。

使用加密就可达到报文鉴别的目的。但在网络的应用中，许多报文并不需要加密。应当使接收者能用很简单的方法鉴别报文的真伪。

1、鉴别的手段

1）报文鉴别（使用报文摘要 **MD (Message Digest)** 算法与数字签名相结合）

2）实体鉴别

九、运输层安全协议

1、 安全套接层 **SSL(Secure Socket Layer)**

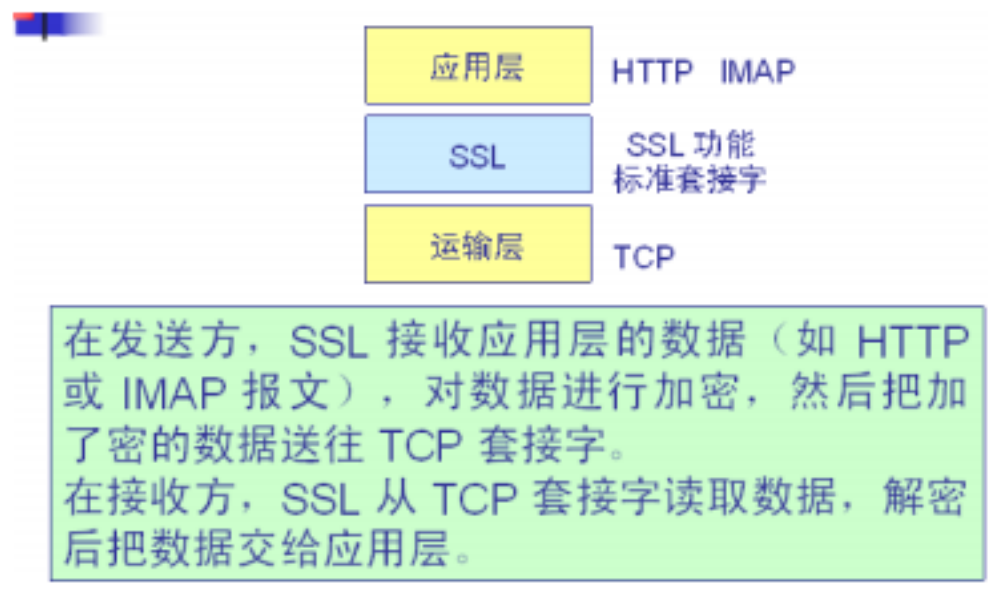
SSL 可对万维网客户与服务器之间传送的数据进行 加密 和 鉴别 。

SSL 在双方的联络阶段协商将使用的加密算法和密钥，以及客户与服务器之间的鉴别。

在联络阶段完成之后，所有传送的数据都使用在联络阶段商定的会话密钥。

SSL 不仅被所有常用的浏览器和万维网服务器所支持，而且也是运输层安全协议 TLS (Transport Layer Security) 的基础。

1.1 SSL 的位置



1.2 SSL 的三个功能：

(1) SSL 服务器鉴别 允许用户证实服务器的身份。具有 SS L 功能的浏览器维持一个表，上面有一些可信赖的认证中心 CA (Certificate Authority) 和它们的公钥。

(2) 加密的 SSL 会话 客户和服务器交互的所有数据都在发送方加密，在接收方解密。

(3) SSL 客户鉴别 允许服务器证实客户的身份。

2、安全电子交易 **SET (Secure Electronic Transaction)**

安全电子交易 SET 是专为在因特网上进行 安全支付卡交易 的协议。

SET 的主要特点是：

(1) SET 是专为与支付有关的报文进行加密的。

(2) SET 协议涉及到三方，即 顾客、商家和商业银行 。所有在这三方之间 交互的敏感信息都被加密 。

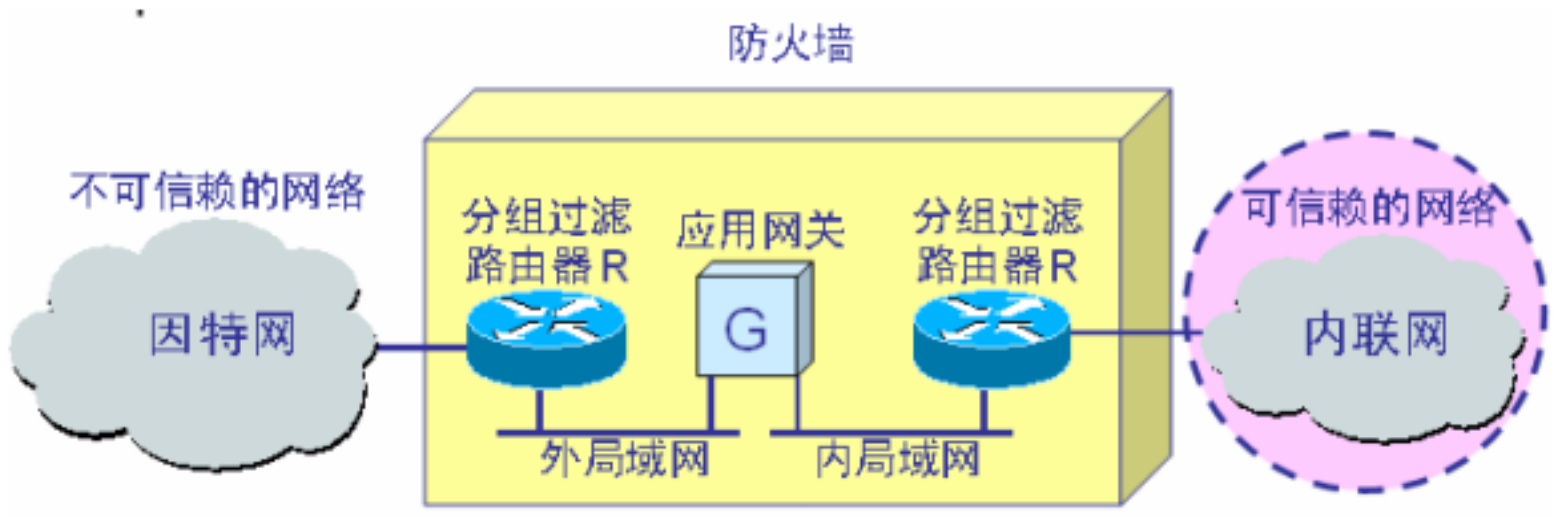
(3) SET 要求这 三方都有证书 。在 SET 交易中，商家看不见顾客传送给商业银行的信用卡号码。

十、防火墙 **(firewall)**

防火墙是由 软件、硬件 构成的系统，是一种 特殊编程的路由器 ，用来在两个网络之间实施接入控制策略。接入控制策略是由使用防火墙的单位自行制订的，为的是可以最适合本单位的需要。

防火墙内的网络称为“ 可信赖的网络 ” (trusted network) ，而将外部的因特网称为“ 不可信赖的网络 ”(untrusted network) 。

防火墙可用来解决内联网和外联网的安全问题。



防火墙在互连网络中的位置

1、防火墙的功能

防火墙的功能有两个： 阻止 和 允许 。

“ 阻止 ” 就是阻止某种类型的通信量通过防火墙（从外部网络到内部网络，或反过来） 。

“ 允许 ” 的功能与 “ 阻止 ” 恰好相反。

防火墙必须能够识别通信量的各种类型。不过在大多数情况下防火墙的主要功能是 “ 阻止 ” 。

2、防火墙技术的分类

(1) 网络级防火墙 ——用来 防止整个网络出现外来非法的入侵 。属于这类的有 分组过滤和授权服务器 。前者检查所有流入本网络的信息，然后拒绝不符合事先制订好的一套准则的数据，而后者则是检查用户的登录是否合法。

(2) 应用级防火墙 —— 从应用程序来进行接入控制 。通常使用 应用网关或代理服务器 来区分各种应用。例如，可以只允许通过访问万维网的应用，而阻止 FTP 应用的通过。

==========

第九章 无线局域网

一、无线局域网的组成

1、有固定基础设施的无线局域网

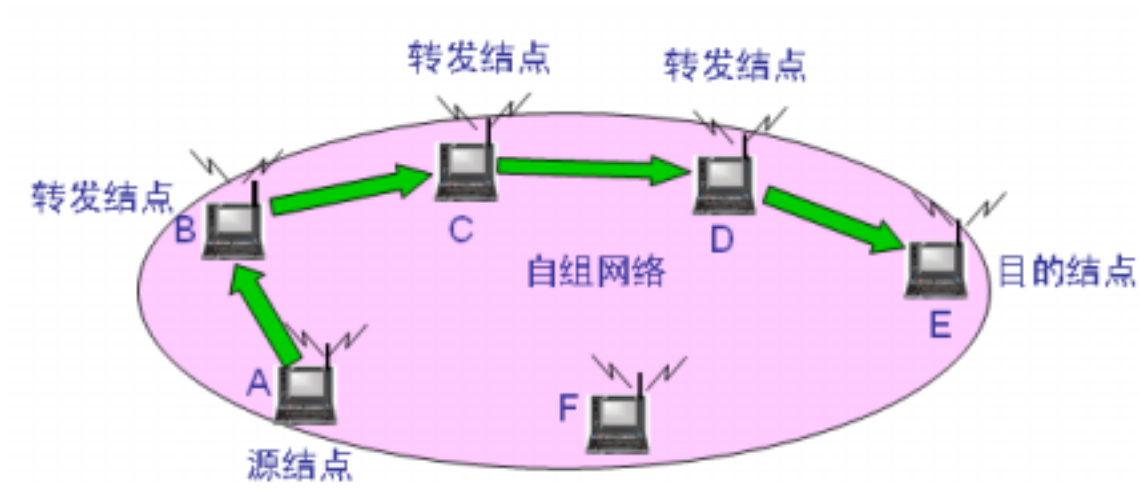
2、无固定基础设施的无线局域网

二、热点 (hot spot)

现在许多地方， 如办公室、 机场、 快餐店、 旅馆、 购物中心等都能够向公众提供有偿或无偿接入 Wi-Fi 的服务。这样的地点就叫做 热点 。

三、移动自组网络，又称自组网络 **(ad hoc network)**

自组网络是 没有固定基础设施 （即没有 AP）的无线局域网。这种网络由一些处于 平等状态 的移动站之间相互通信组成的 临时网络：



四、 **802.11** 局域网的 **MAC** 帧

802.11 帧共有三种类型，即 控制帧 、 数据帧 和管理帧 。

==========

第十章 下一代因特网

一、 IPv6 的基本首部

IPv6 仍支持 无连接 的传送所引进的主要变化如下

更大的地址空间。 IPv6 将地址从 IPv4 的 32 位 增大到了 128 位。

扩展的地址层次结构。

灵活的首部格式。

改进的选项。

允许协议继续扩充。

支持 即插即用（即自动配置）

支持资源的预分配。

IPv6 将首部长度变为固定的 40 字节，称为基本首部 (base header)。

将不必要的功能取消了，首部的字段数减少到只有 8 个。

取消了首部的检验和字段，加快了路由器处理数据报的速度。

在基本首部的后面允许有零个或多个扩展首部。

所有的扩展首部和数据合起来叫做数据报的有效载荷 (payload)或净负荷。

二、 从 IPv4 向 IPv6 过渡

向 IPv6 过渡只能采用逐步演进的办法， 同时，还必须使新安装的 IPv6 系统能够向后兼容。

IPv6 系统必须能够接收和转发 IPv4 分组，并且能够为 IPv4 分组选择路由。

双协议栈 (dual stack)是指在完全过渡到 IPv6 之前，使一部分主机（或路由器）装有两个协议栈，一个 IPv4 和一个 IPv6。